

Intelligent Video Surveillance Server

Configuration Guide

V1.1.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Regulatory Information

FCC Information



Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

- For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help.

General

This configuration guide (hereinafter referred to be "the Guide") introduces the face recognition arming operations of the Intelligent Video Surveillance Server device (IVSS device) (hereinafter referred to be "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Writing Conventions

In order to simplify the description, the commonly used functional names in this guide are made as follows.

- Without otherwise specified, the Device in this guide refers to the IVSS device.

- The remote device in this guide refers to the front-end device such as IPC and speed dome connected to the IVSS device via the network.
- The AI Module in this guide refers to the AI card installed in the IVSS device.
- To guarantee the security of personal privacy, the private information such as human face and car plate number has been dealt with.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	April, 2018
2	V1.0.1	Add privacy protection notice.	May, 2018
3	V1.1.0	• Update Model list. • Update some contents and relevant interface pictures. • Improve structure and some description.	Sept, 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.

- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Read the guide carefully before use to prevent danger and property loss. Strictly conform to the guide during application and keep it properly after reading.

Operating Requirement

- Don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Don't install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Don't dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used.
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Make sure to use standard power adapter matched with this device. Otherwise, the user shall undertake resulting personnel injuries or device damages.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Points for Attention:

AI module does not support hot plug. If you need to replace the AI module, unplug the device power cable first. Otherwise, it will lead to file damage on the AI module.

Table of Contents

Cybersecurity Recommendations	I
Regulatory Information.....	III
Foreword	IV
Important Safeguards and Warnings	VII
1 Overview.....	1
1.1 Introduction	1
1.2 Configuration Notes.....	1
1.3 Configuration Procedure	1
2 Application Scenario.....	3
3 Installation and Connection	7
3.1 Installing IPC.....	7
3.1.1 Site Requirements	7
3.1.2 Light	7
3.1.3 Installation Rules	10
3.1.4 Installation Guide	10
3.1.5 Lens Options.....	12
3.1.6 Installation Effect	13
3.2 Installing IVSS	15
3.2.1 Installing HDD	15
3.2.2 Installing AI Module.....	17
3.2.3 Connecting Cables	20
4 Initial Configurations	22
4.1 Initializing IVSS Device	22
4.2 Quick Settings	24
4.2.1 System Time Settings	24
4.2.2 IP address Settings.....	25
4.2.3 P2P	27
4.3 IPC Settings.....	31
4.3.1 Initializing IPC	32
4.3.2 Enabling Human Face Detection.....	38
4.3.3 Configuring Human Face Detection	39
4.4 Registering IPC	40
4.4.1 Short-Cut Menu	40
4.4.2 Manual Adding	45
5 Face Recognition Arming	48
5.1 Procedure	48
5.2 Configuring Human Face Database.....	48
5.2.1 Creating Human Face Database.....	48
5.2.2 Adding Human Face Image	51
5.2.3 Human Face Modeling	57
5.3 Enabling AI Plan	59

5.4 AI Display Settings.....	60
5.5 Human Face Detection Settings.....	63
5.6 Face Recognition Settings	66
6 Configuration Results.....	70
6.1 Preview Monitor.....	70
6.1.1 Structured Display	70
6.1.2 Image Preview	71
6.2 Playback Control	72
6.2.1 Record Playback.....	72
6.2.2 Image Playback	77
6.3 Searching by Face Image	79
7 FAQ	83

1.1 Introduction

Intelligent Video Surveillance Server (IVSS) is a product of new form. Compatible with the general functions of video surveillance of security industry, it has added AI functions such as human face recognition and feature extraction based on the deep learning technology. This guide introduces the arming operations of IVSS face detection and face recognition, including operations such as application scenario, device installation, preparation and configurations. It supports AI detection functions by camera or by device, such as face detection and face recognition.

- AI by camera: The remote device such as smart IPC supports smart detection. The Device only needs to support to detect and display the smart alarm information from the remote device, and perform smart detection configuration and record playback for the remote device.
- AI by device: The remote device does not support AI analysis and the IVSS device performs intelligent detection for the remote device.

1.2 Configuration Notes

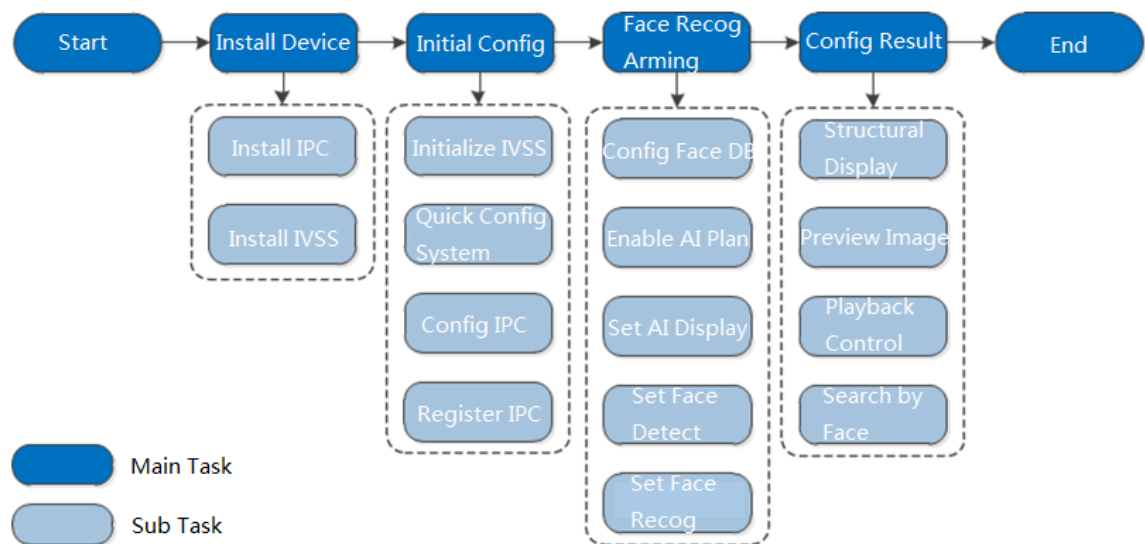
It is recommended that the configuration personnel master the basic IVSS operation skills. For basic operations, see *User's Manual*.

IVSS device supports local, Web and IVSS browser operations. The steps and interfaces in this guide are mainly based on local operations. There might be some differences when operating on the Web and IVSS browsers. The actual interface shall prevail.

1.3 Configuration Procedure

See Figure 1-1 for the IVSS face arming procedure.

Figure 1-1 Configuration procedure



2

Application Scenario

Face detection and face recognition are suitable for the important entrance/exit and security checkpoint in subway, rail station and bus station.

Main Entrance of Public Places

For public places such as shopping mall, canteen and Internet café, it is required to have two doors at the entrance/exit. The IPC is installed indoor directly facing the gate. It is not directly exposed to the outside scene and is suitable for face snapshot. See Figure 2-1.

Figure 2-1 Main entrance of public places



Deprecated scenario: Doorway with direct sunlight or backlight scenario which causes the face to be dim. See Figure 2-2.

Figure 2-2 Deprecated scenario



Security Checkpoint

In the security channels of public transportation such as highway, railway and airport, people pass one by one and the flow direction is consistent, which is a suitable scene for face snapshot. See Figure 2-3.

Figure 2-3 Security checkpoint in highway station/airport



Deprecated scenario: Background with serious backlight. The security checkpoint is directly set at the entrance and forms a strong WDR scene. See Figure 2-4. The effect of face snapshot in this scene is poor (the light changes obviously at different time periods throughout the day and the snapshot effect also changes much).

Figure 2-4 Deprecated scenario



Ticket Gate

At the ticket gate in railway station or subway, people pass the gate one by one and the flow direction is consistent, which is a suitable scene for face snapshot. See Figure 2-5.

Figure 2-5 Ticket gate



Deprecated scenario: There are billboards with strong light on the back or side wall. Backlight scene is easy to cause the face to be dim. See Figure 2-6.

NOTE

Avoid installing ticket gates in front of billboards.

Figure 2-6 Deprecated scenario



3.1 Installing IPC

The IPC installation site and installation mode affects the general effect of face detection and face recognition. This chapter mainly introduces the requirements on IPC installation site and brightness, and gives guidance on installation.

For detailed operations to install the IPC, see *IPC User's Manual*.

3.1.1 Site Requirements

- Network

Network is available at the site to enable IPC transmitting real-time video stream to the IVSS device. IPC bandwidth shall be more than 6 Mbps and transmission delay shall be less than 1 second.

- Power supply

Power supply at the site can meet the IPC requirements.

- Construction

Construction conditions are ready at the site.

3.1.2 Light

This section introduces the light requirements and strategies to improve the light condition.

3.1.2.1 Light Requirements

The light at the IPC installation site shall meet the following three conditions:

- The illumination of pedestrian front face shall be above 100lux.

If the illumination cannot meet the requirement (such as night or daytime without enough light), it will lead to insufficient face exposure and causes the captured image to have more noises and be dim. See Figure 3-1.

Figure 3-1 Insufficient face exposure



- The illumination of pedestrian side face shall be 100lux to 200lux. The difference between the left and right sides shall be less than 1 time of the smaller one.

If the illumination difference between the left and right sides is too bigger, it will cause the face to be bright on one side and dim on the other. See Figure 3-2.

Figure 3-2 Bright on one side and dim on the other



- $\text{Illumination at the back} < \text{Illumination on the front} \times 2$

If the illumination at the back is larger than twice of that on the front, it will lead to serious backlight on the captured face and cause the image to be insufficient exposure and unclear. See Figure 3-3.

Figure 3-3 Backlight face



3.1.2.2 Improving Light Condition

If the light condition at the site does not meet the requirements specified in "3.1.2.1 Light Requirements," you need to improve the light condition through wide dynamic range (WDR) or fill light.

- Wide dynamic range (WDR)
WDR can help to improve phenomena of backlight and sharp light contrast on the face.
- Fill light

Improve illumination by adding extra light to improve the face collection effect. It mainly uses ordinary spotlight or incandescent lamp to improve the face illumination and avoid sharp illumination contrast on the captured image. See Figure 3-4.

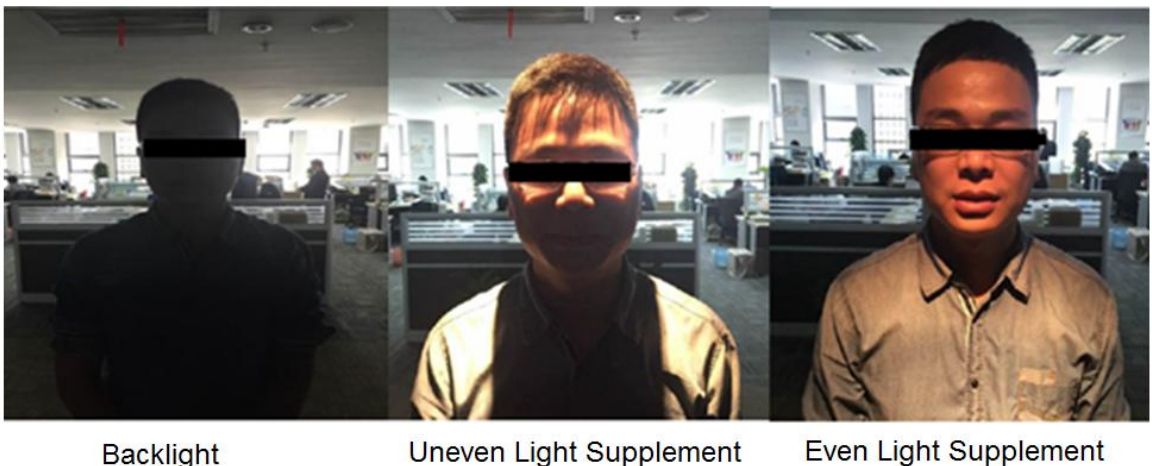
Figure 3-4 Fill light



Points for attention when installing the fill light:

- ◇ Avoid uneven light supplement
Improper fill light angle or intensity will cause uneven light on the face. For example, vertical installation of intense light will cause uneven face illumination, which highlights the forehead and shadows the eye sockets. See Figure 3-5.
If allowed, it is recommended to use light of diffuse reflection (light without certain direction).

Figure 3-5 Fill light effects



- ◇ Set light according to different time periods

In some scenarios, the light condition changes much from daytime to the night and sunny to cloudy. The illumination difference and backlight will switch to insufficient light at night. So you shall change the method of light-fill accordingly and debug the best light-fill time.

- ◇ Be flexible according to the actual situation

In the absence of light (at night), the effect of fill light cannot be better than the lighting lamp. A separate fill light is easy to cause uneven light supplement. Due to the light limitation, currently there is no face system with good effect available which can be used outdoors at night.

- ◇ Avoid shooting directly at the eyes of pedestrians

If the fill light shoots at the eyes of the pedestrian directly, the pedestrian will block the light with the hand and face snapshot will be affected. When installing a fill light, add a layer outside the light to reduce the light intensity and avoid direct exposure to people's eyes.

3.1.3 Installation Rules

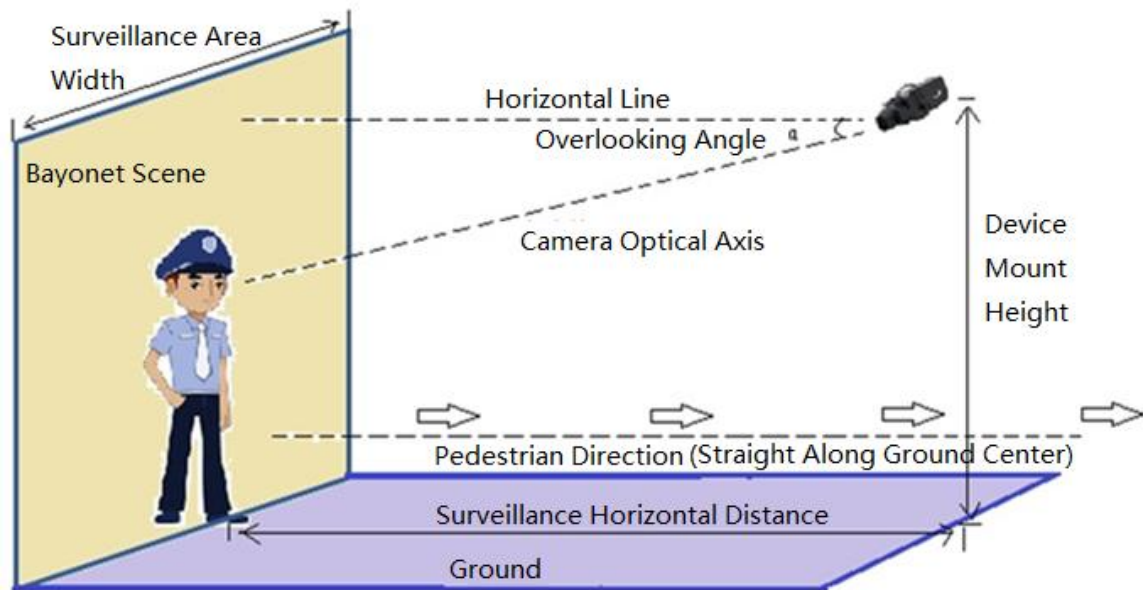
IPC installation rules are listed as follows (including but not limited to):

- Bright indoor environment (illumination $\geq 100\text{lux}$). Never use environment with strong backlight (such as facing the gateway).
- Consistent flow direction (avoiding crossing) and avoid side face.
- Even illumination. Keep away from environment with billboard on one side to avoid uneven illumination on the face.
- Easy to install the IPC (normal mounting height: 2.5m – 3m). Keep the snapshot distance from 2.5 meters through 3 meters.
- Avoid outdoor environment. If it is necessary to install the IPC outdoors, the preferred direction is from north to south (avoiding strong backlight or front light). It is recommended to set the snapshot point at sidewalk shielded by trees and keep the width of the monitored road within 3 meters.

3.1.4 Installation Guide

The main function of IPC is to obtain high quality front face images and avoid face tampering when personnel passing back and forth. For the IPC installation principle and effect, see Figure 3-6.

Figure 3-6 IPC installation effect map

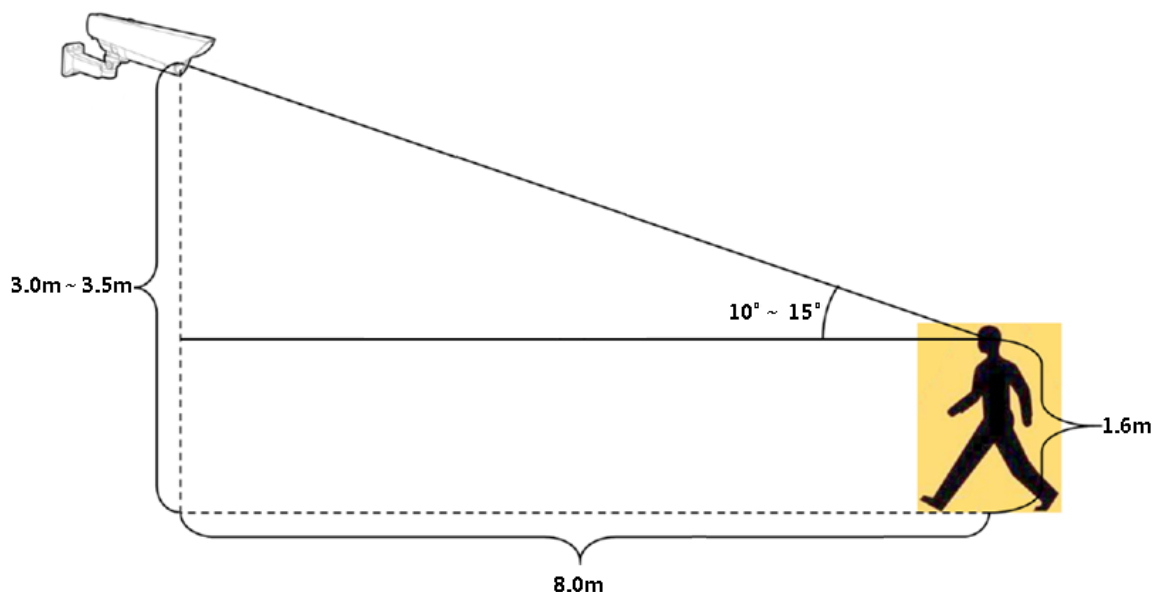


Make sure the installation meets the following requirements:

- Install IPC in front of the channel to capture the front face. Keep the face shifting leftward or rightward $<30^\circ$ and shifting upward or downward $<15^\circ$. Therefore, instead of side mount, you shall select ceiling mount or front mount with a connection pole.
- The width of the monitoring area is the width of the IPC shooting area. You need to select different types of IPC and lens according to different shooting width.
- The recommended IPC mounting height is 2.5m to 3m, and the recommended IPC monitoring horizontal distance is 7m to 10m.
- Overlooking angle $\alpha < 15^\circ$.
- Keep level of the image. Remain the snapped object in the center of the image.

For the IPC installation physical parameters, see Figure 3-7.

Figure 3-7 IPC installation physical parameters



Suppose that the personnel height is 1.7m (1.6m in the figure refers to the height from the eyes to the ground). When the horizontal distance from the IPC to the human face is 8.0m, and the overlooking angle from IPC to the face is from 10° through 15°, the IPC height shall be from 3.0m through 3.5m. If the overlooking angle is too small (such as lens parallel to the face), it will cause serious face tampering. If the overlooking angle is too large, it will cause face deformation.

3.1.5 Lens Options

According to different widths of monitoring areas, it is recommended to select different IPCs. For details, see Table 3-1.

Table 3-1 IPC options

Monitoring Area Width (m)	Recommended IPC	Lens Option
<3m	200W pixel IPC	For details, see "3.1.5.1 200W Pixel IPC."
3m<Width<5m	800W pixel IPC	For details, see "3.1.5.2 800W Pixel IPC."
>5m	Recommend to use multiple IPCs	For details, see "3.1.5.3 Installing multiple IPCs."

NOTE

The following contents are for reference only. You shall select the suitable IPC and lens according to the actual site needs.

3.1.5.1 200W Pixel IPC

When the actual width of the monitoring area is less than 3m, it is recommended to install the 200W pixel IPC. You need to select the lens model according to the monitoring horizontal distance and installation height of IPC. For details, see Table 3-2.

Table 3-2 Lens options (200W IPC)

Monitoring Horizontal Distance (m)	Mounting Height (m)	Lens (mm)	Lens Model	Overlooking Angle
5	2	10.5-42	OPT-117F10542D-IR12MP	10°
7	2.5	10.5-42	OPT-117F10542D-IR12MP	10°
8	2.8	10.5-42	OPT-117F10542D-IR12MP	10°
9	3	10.5-42	OPT-117F10542D-IR12MP	10°
12	3.5	15-75	OPT-117C1575D-IR12M	10°

3.1.5.2 800W Pixel IPC

When the actual width of the monitoring area is more than 3m and less than 5m, it is recommended to install the 800W pixel IPC. You need to select the lens model according to the monitoring horizontal distance and installation height of IPC. For details, see Table 3-3.

Table 3-3 Lens options (800W IPC)

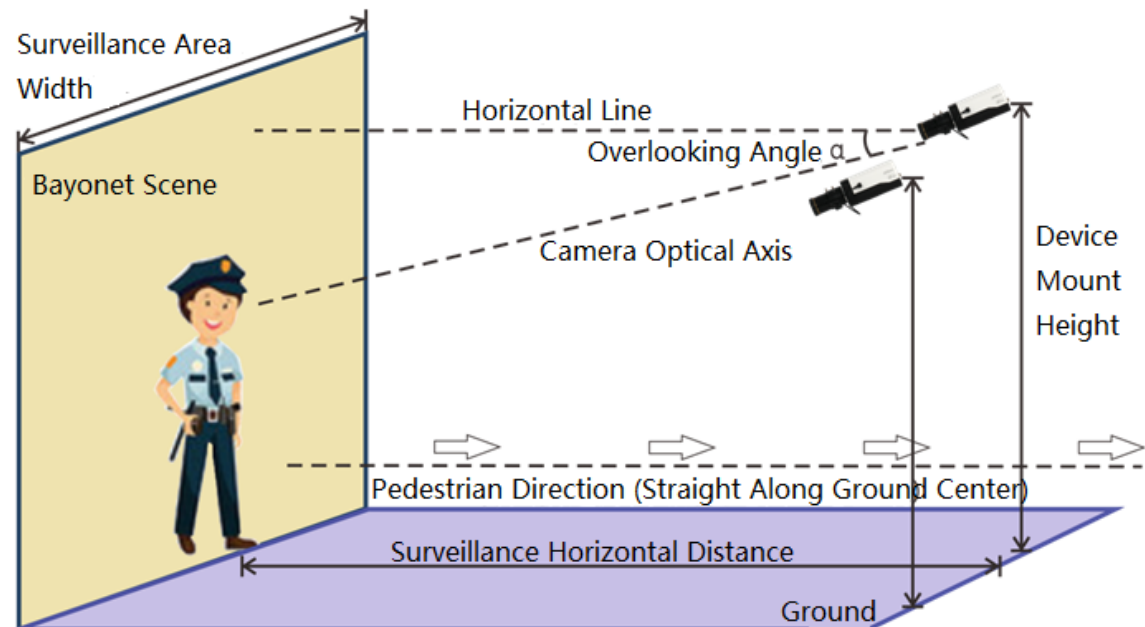
Monitoring Horizontal Distance (m)	Mounting Height (m)	Lens (mm)	Lens Model	Overlooking Angle
------------------------------------	---------------------	-----------	------------	-------------------

Monitoring Horizontal Distance (m)	Mounting Height (m)	Lens (mm)	Lens Model	Overlooking Angle
5	2	3.7~16	OPT-117F3716D-IR12MP	10°
7	2.5	3.7~16	OPT-117F3716D-IR12MP	10°
8	2.8	3.7~16	OPT-117F3716D-IR12MP	10°
9	3	10.5~42	OPT-117F10542D-IR12MP	10°
12	3.5	10.5~42	OPT-117F10542D-IR12MP	10°
20	5	15~75	OPT-117C1575D-IR12M	10°

3.1.5.3 Installing multiple IPCs

When the actual width of the monitoring area is more than 5m, it is recommended to install multiple IPCs. The effect is shown as in Figure 3-8. You need to select the lens model according to the monitoring horizontal distance and installation height of IPC. For details, see "3.1.5.1 200W Pixel IPC" and "3.1.5.2 800W Pixel IPC".

Figure 3-8 Installation effect map (multiple IPCs)

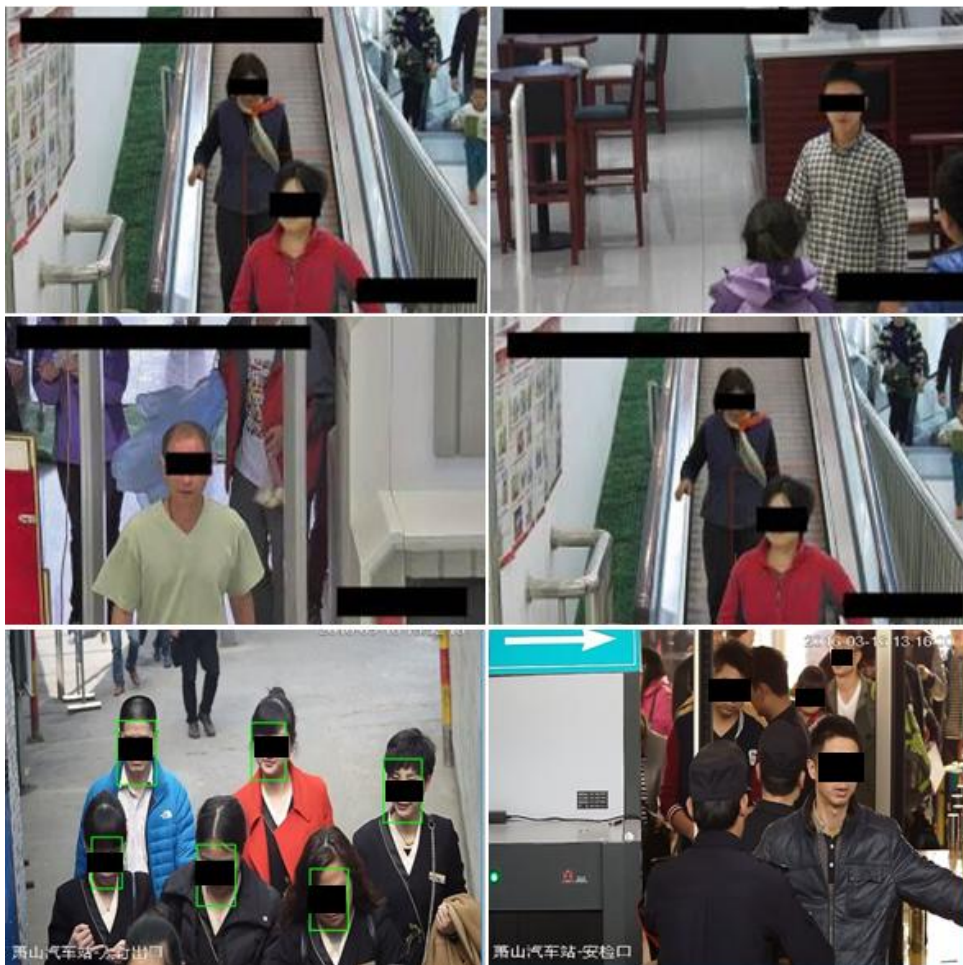


3.1.6 Installation Effect

After IPC installation, you can log in the IPC Web interface to view shooting effect and debug IPC image parameters. For details, see *IPC User's Manual*.

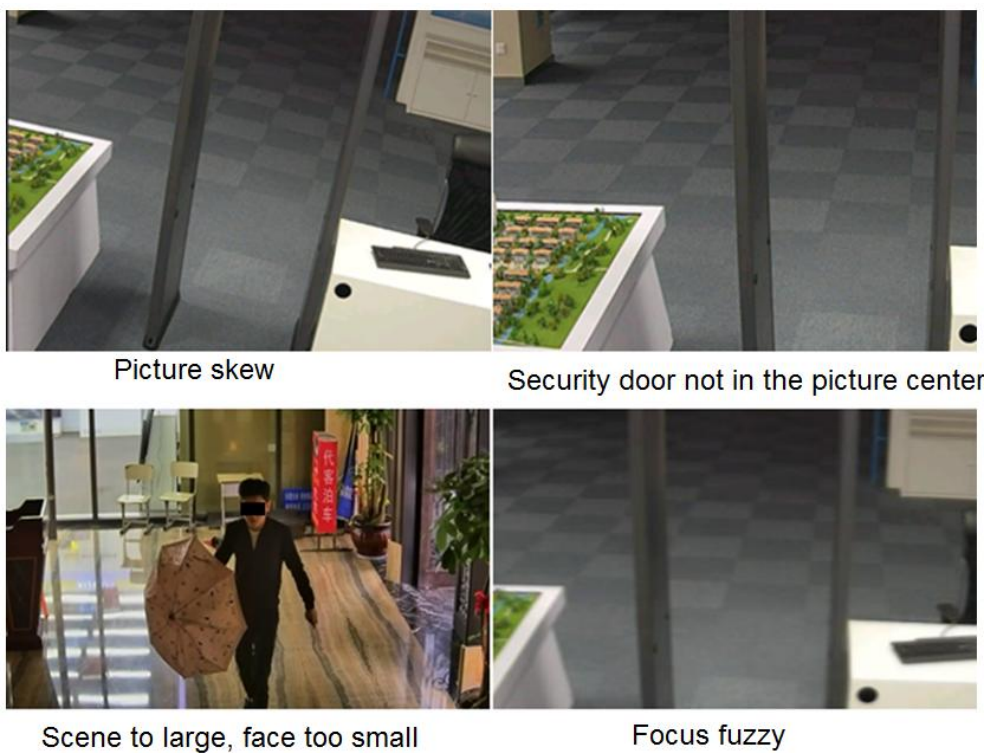
- For correct installation sample, see Figure 3-9.

Figure 3-9 Correct sample



- For incorrect installation sample, see Figure 3-10.

Figure 3-10 Incorrect sample



3.2 Installing IVSS

The section introduces HDD installation and cable connection.



WARNING

Part of the device is heavy. Carry with several persons to avoid any personnel injury.

3.2.1 Installing HDD

The section introduces the detailed operations to install the HDD.



NOTE

Different models support different HDD numbers. See the actual situation.

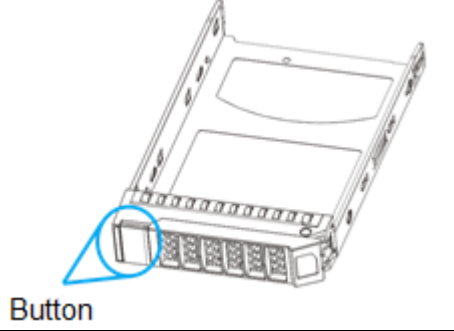
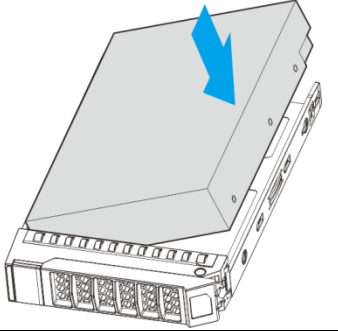
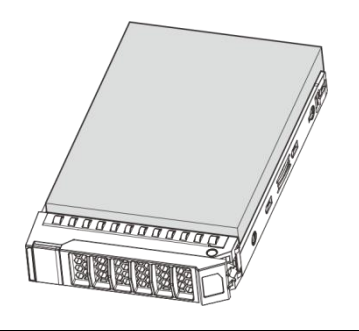
3.2.1.1 12-HDD



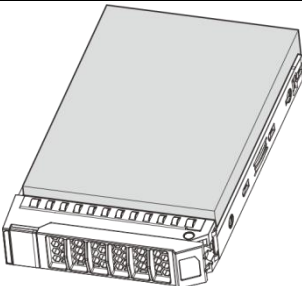
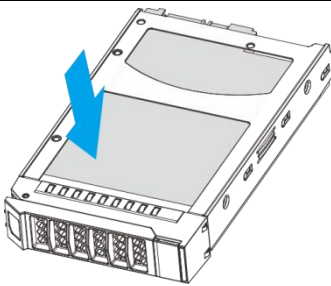
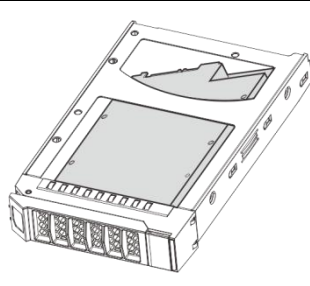
CAUTION

If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

Installing HDD

 Button		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the empty HDD box.	② Place one side of the HDD closely along the upper side of the box and press down to push the HDD down to the lower side of the mounting surface.	③ Insert the HDD box into the HDD slot, press it to the bottom, and then close the box handle.

Removing HDD

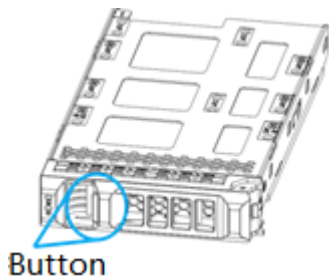
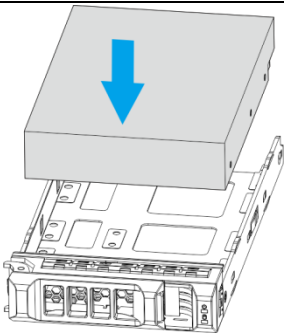
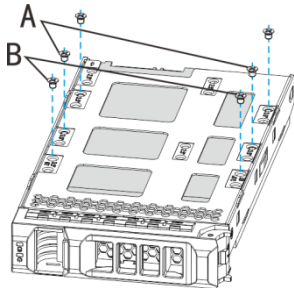
		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	② On the back of the HDD box, press hard on the position indicated by the arrow.	③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.

3.2.1.2 16/24-HDD

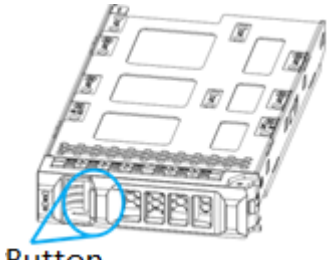
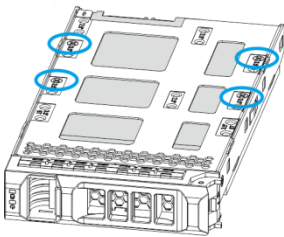
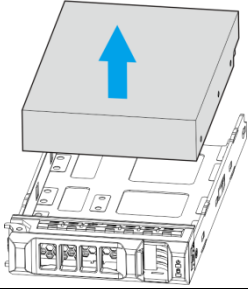


If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

Installing HDD

 Button		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the empty HDD box.	② Put the HDD into the box along the direction shown in the figure.	③ Lock the screws on the back of the HDD box. Insert the box into the HDD slot, push it to the bottom, and then close the handle.  NOTE In the figure, you only need to lock one set of the screws (Group A or Group B). See the actual situation.

Removing HDD

 Button		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	② Unlock the screws on the back of the HDD box.  NOTE The screws are at different positions for different HDDs. See the actual situation.	③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.

3.2.2 Installing AI Module

The Device supports to install AI module to realize smart detective functions such as face detection and face recognition. You can view the running status of the AI module from the corresponding indicator on the rear panel.

AI module is not the standard accessory. You can purchase it according to actual needs.

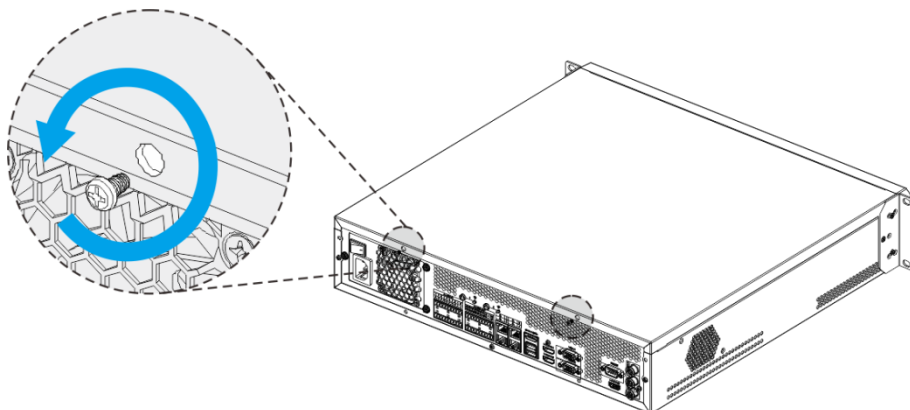


CAUTION

- The following contents apply to devices of 8-HDD and 12-HDD only.
- The following figures are for reference only. The actual product shall prevail.
- Devices of different models support different numbers of AI modules. See the actual situation.
- AI module does not support hot plug. If you need to replace the AI module, unplug the device power cable first. Otherwise, it will lead to file damage on the AI module.

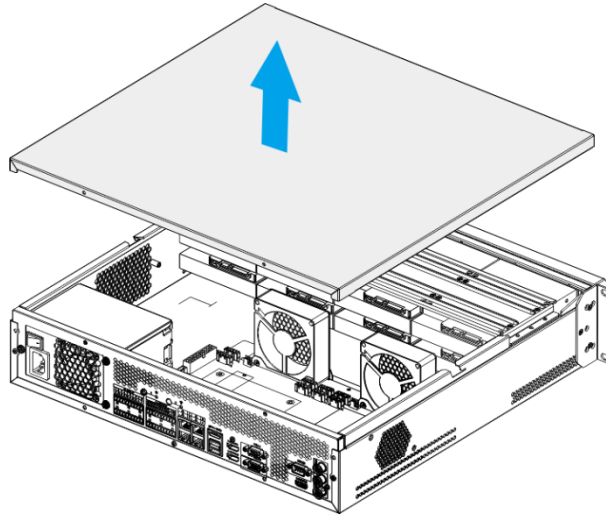
Step 1 Remove the screws on the rear panel of the Device. See Figure 3-11.

Figure 3-11 Install AI module (1)



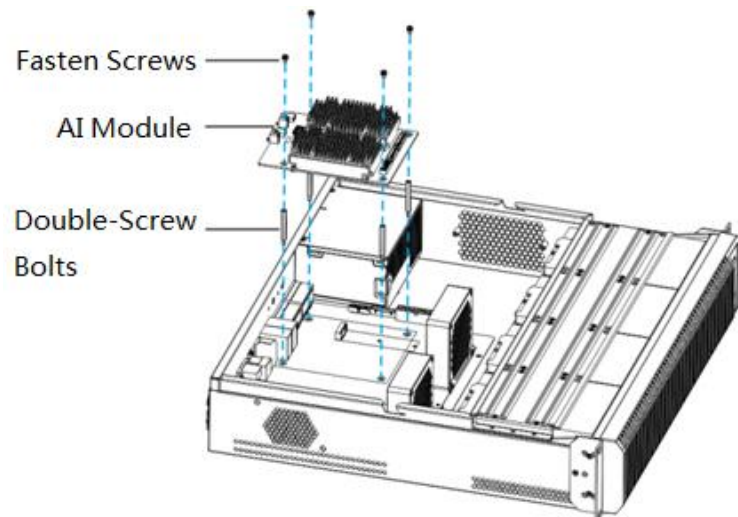
Step 2 Remove the case cover. See Figure 3-12.

Figure 3-12 Install AI module (2)



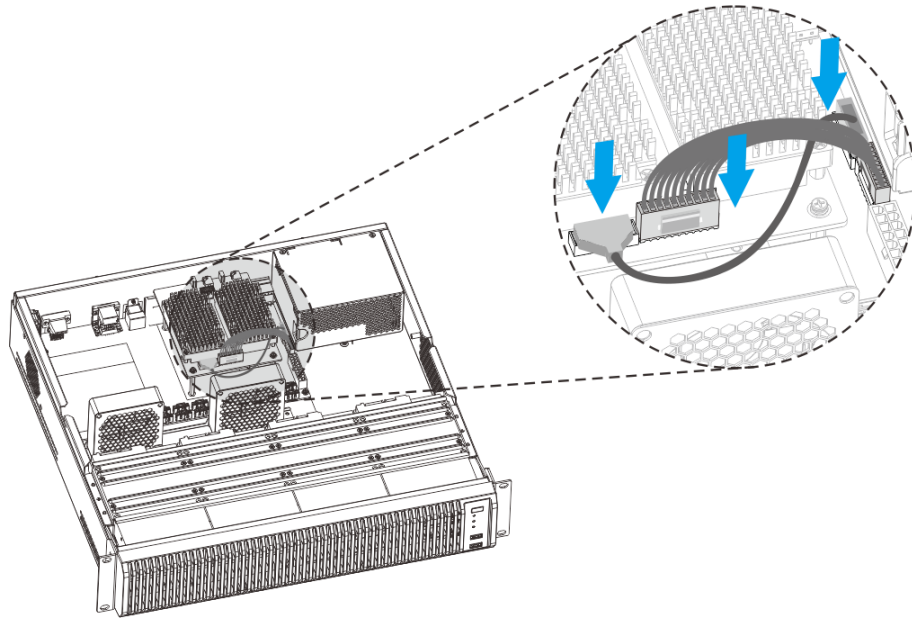
Step 3 Install the double-screw bolts and AI module and then fasten the screws. See Figure 3-13.

Figure 3-13 Install AI module (3)



Step 4 Connect the power cable and data cable of the AI module. See Figure 3-14.

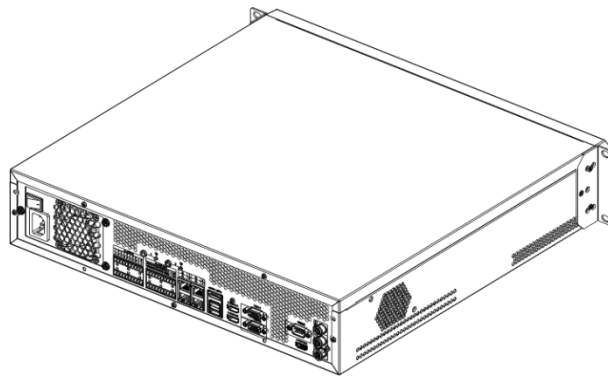
Figure 3-14 Install AI module (4)



Step 5 (Optional) Install the rest AI modules according to Step 3 to Step 4.

Step 6 Put back the cover and fasten the screws on the rear panel. See Figure 3-15.

Figure 3-15 Install AI module (5)



Step 7 Check AI module version.

- 1) Turn on the Device.
- 2) Click  on the **LIVE** interface and select **MAINTAIN > Device Maintain > Upgrade**.
- 3) Click the Host tab and AI Module tab respectively to check if the host version matches with the AI module version. See Figure 3-16 and Figure 3-17.
If the version is not matched, you need to upgrade the host. For details, see *IVSS User's Manual*.

Figure 3-16 Host upgrade

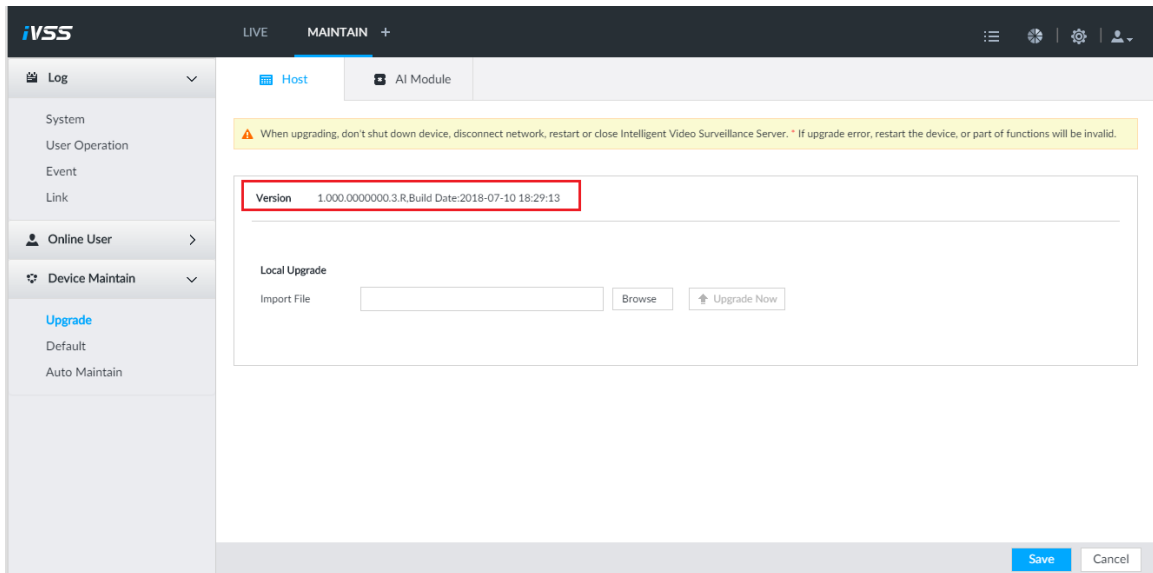
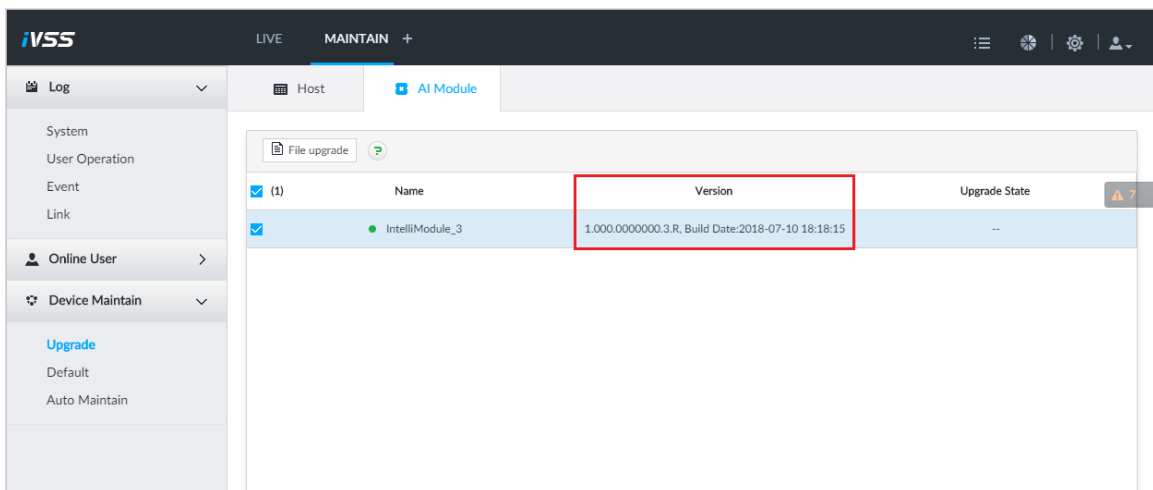


Figure 3-17 AI module upgrade

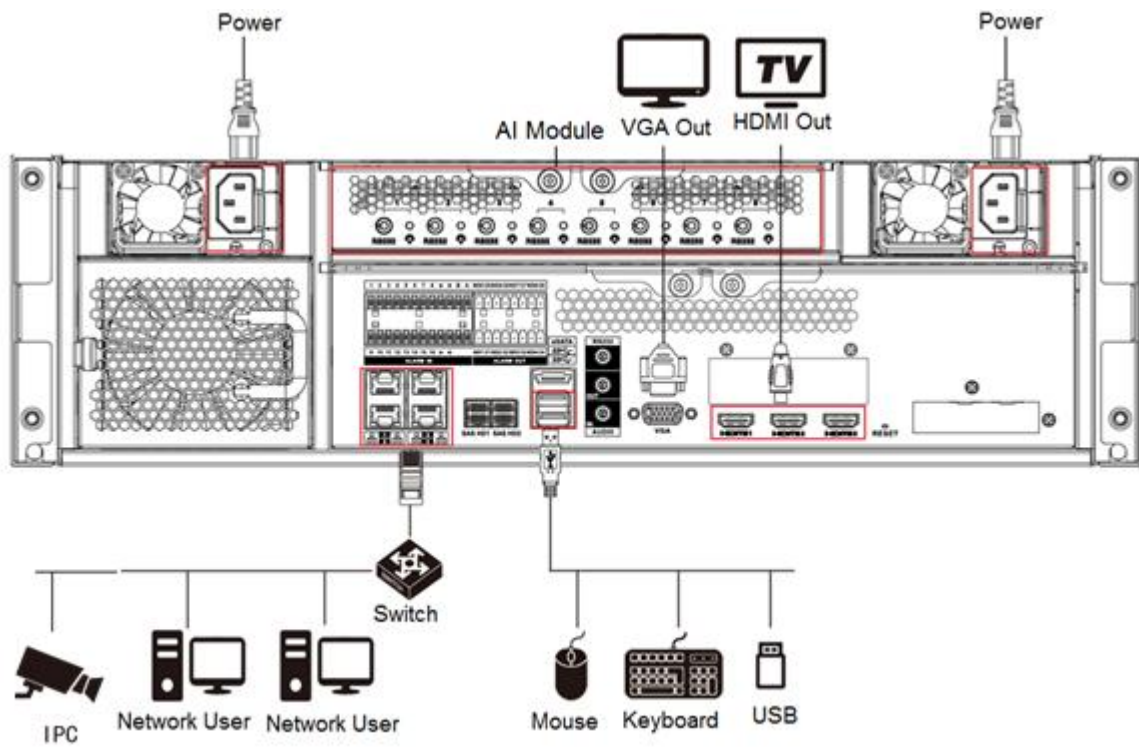


3.2.3 Connecting Cables

For the device connection, see Figure 3-18. The following figure is for reference only. The actual product shall prevail.

- Display, mouse and keyboard are needed for local operation.
- The device supports to install AI module to realize smart detective functions such as face detection and face recognition. You can view the running status of the AI module from the corresponding indicator on the rear panel.

Figure 3-18 Connection



4 Initial Configurations

Before configuring face recognition, you need to configure the IVSS device and IPC.

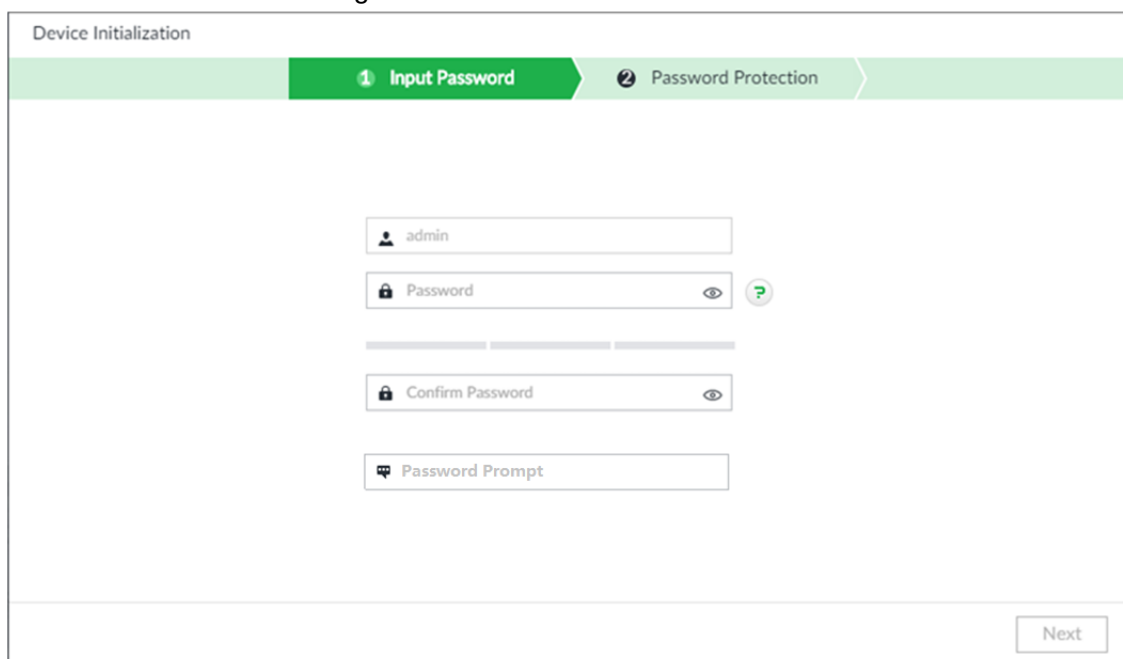
4.1 Initializing IVSS Device

When booting up for the first time or restoring factory defaults, you need to configure the password information for **admin** (by default). You can also set password protection methods according to practical needs.

Step 1 Turn on the Device.

The **Device Initialization** interface is displayed. See Figure 4-1.

Figure 4-1 Device initialization



Step 2 Configure the admin password. For details, see Table 4-1.

Table 4-1 Description of password setting parameters

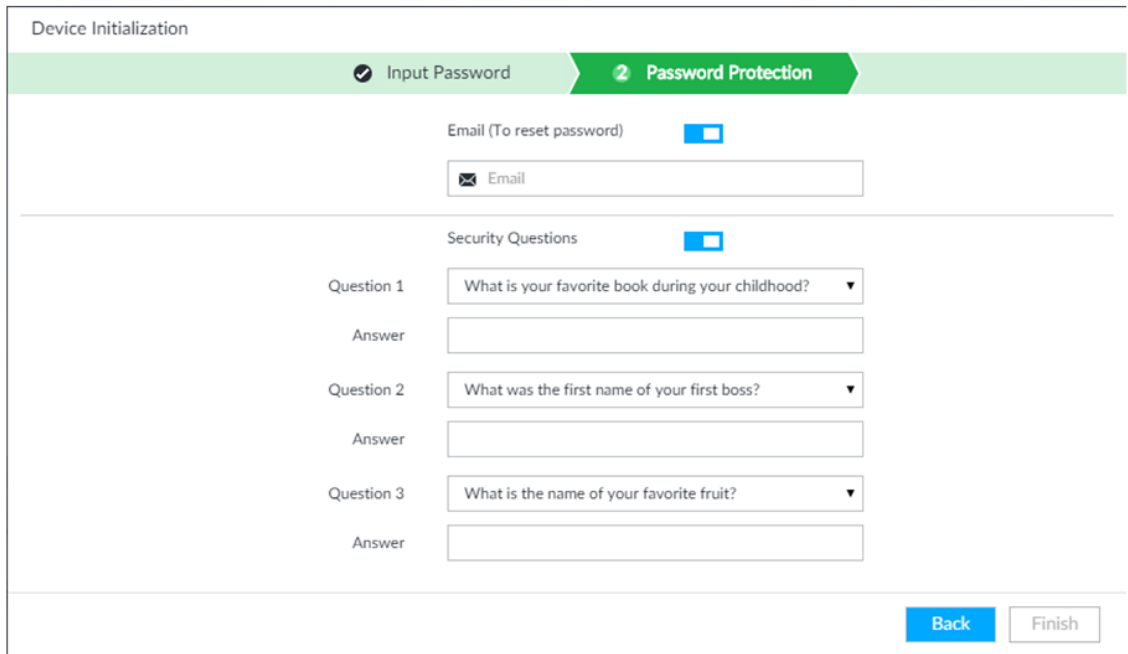
Parameter	Description
User	The default user is admin.
Password	The password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special character (excluding "", "", ":", "." and "&"). It is recommended to set a password of high security according to the prompt.
Confirm Password	 NOTE After entering the password, press and hold down  with the mouse to display the password characters. Release the mouse or move the cursor to other position, the password is displayed at hidden mode again.

Parameter	Description
Password Prompt	After setting the prompt, when you move the mouse to  on the login interface, the system pops up the prompt to help you remember the password.  NOTE Only the local interface supports password prompt. See the actual interface.

Step 3 Click **Next**.

The password protection setting interface is displayed. See Figure 4-2.

Figure 4-2 Password protection



Step 4 Configure the password protection. For details, see Table 4-2.

After setting the password protection, if you forgot the admin password, you can reset it via the reserved email or answering the security questions. For details, see *User's Manual*.

 **NOTE**

Click  to disable reserved email and security questions.

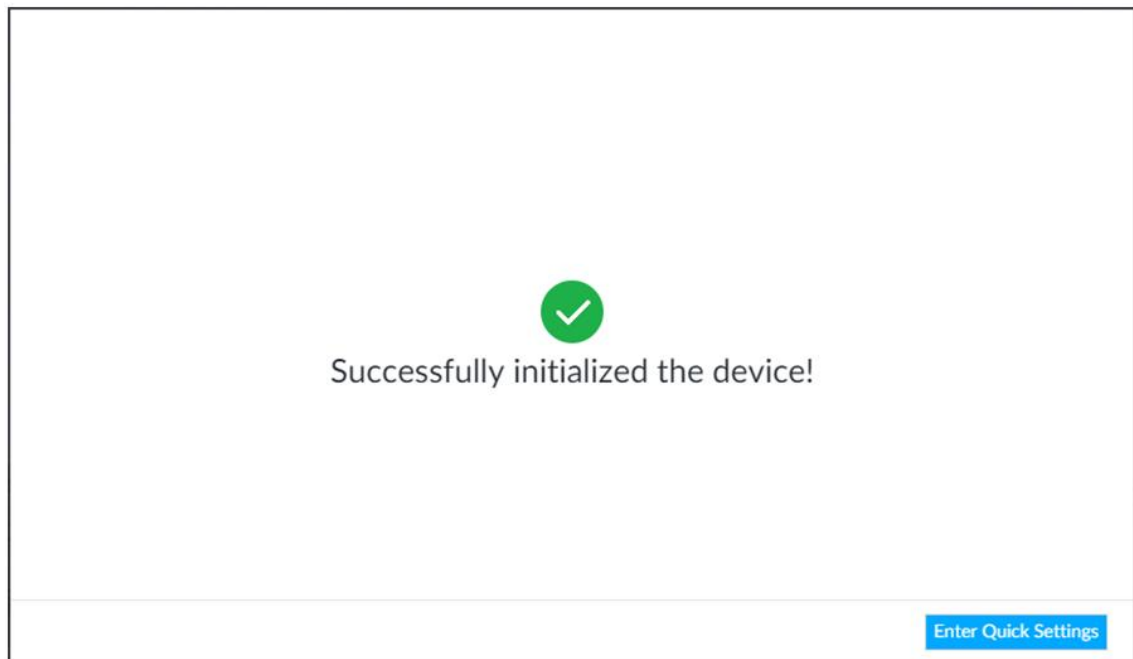
Table 4-2 Description of password protection

Protection Method	Description
Email	Enter the reserved email address. Scan the QR code, enter the security code received in the reserved email, and then you can reset the password. You can modify the reserved email in the Property interface. For details, see <i>User's Manual</i> .
Security Questions	Select the security questions and enter the answers. You can answer the questions to reset the admin password.

Step 5 Click **Finish** to complete the device initialization.

The interface shows **Successfully initialized the device!** See Figure 4-3. Click **Enter Quick Settings** to configure the device basic information. For details, see "4.2 Quick Settings."

Figure 4-3 Successfully initialized



4.2 Quick Settings

After the device initialization, you can enter the Quick Settings interface to configure the system time, IP address and P2P.

4.2.1 System Time Settings

Set the device system time. You can select to enable NTP or not according to practical needs. If NTP is enabled, the system automatically syncs time with the NTP server.

Step 1 Click **Enter Quick Settings** on the successful initialization interface.

The time setting interface is displayed. See Figure 4-4.

Figure 4-4 Time setting

Step 2 Configure the parameters. For details, see Table 4-3.

Table 4-3 Description of system time parameters

Parameter	Description
Time	Configure the system date and time. You can choose manual setting or auto sync to NTP server. - Manual Setting: Select the Manual Setting check box and configure the date and time according to practical situation. - Sync with Internet Time Server: Select the Sync with Internet Time Server check box, enter the IP address or domain name of the NTP server, and then enter the time interval.
Time and Date Format	Select the display format of system date and time.
Time Zone	Select the time zone that the Device locates.

Step 3 Click **Next** to save the configuration.

4.2.2 IP address Settings

Modify device information such as IP address and DNS server according to the network plan.

NOTE

There are four Ethernet ports available. Make sure that at least one port is connected to the network before setting the IP address.

Step 1 Click **Next** on the time setting interface.

The IP setting interface is displayed. See Figure 4-5.

Figure 4-5 IP setting

Quick Configuration

Time **2 IP Set**

NIC	NIC Type	Dhcp	IP Address	Subnet Mask	Mac	Speed	Operate
Ethernet ...	Electric Port	No	192.168.2.108	255.255.255.0	34:22:3d:da:32...	10M/100MSeL...	
Ethernet ...	Electric Port	No	192.168.3.108	255.255.255.0	34:22:3d:da:32...	10M/100MSeL...	
Ethernet ...	Electric Port	No	192.168.4.108	255.255.255.0	34:22:3d:da:32...	10M/100MSeL...	

DNS Server

☐ Obtain DNS server address automatically

☒ Use the following DNS server address

Preferred DNS: 8 . 8 . 8 . 8

Alternate DNS: 8 . 8 . 4 . 4

Default NIC

Default Ethernet: Ethernet Network1

Back Next

Step 2 Configure the IP address.

- 4) Click corresponding to the Ethernet port.

The **Edit Ethernet Network 1** interface is displayed. See Figure 4-6.

Figure 4-6 Editing Ethernet network

Edit Ethernet Network1

Speed: 1000 Mb/s

☐ Use Dynamic IP Address

☒ Use Static IP Address

Static IP Address: 192 . 168 . 3 . 108

Subnet Mask: 255 . 255 . 0 . 0

Gateway: 192 . 168 . 0 . 1

MTU: 1500

OK Cancel

- 5) Configure the parameters. For details, see Table 4-4.

Table 4-4 Description of NIC editing parameters

Parameter	Description
Speed	The max network transmission speed of the current NIC.
Use Dynamic IP Address	When there is a DHCP server in the network, select this check box and the system can allocate a dynamic IP address to the Device. There is no need to set IP address manually.

Parameter	Description
Use Static IP Address	Select the check box and enter the static IP address, subnet mask and gateway. It is to set a static IP address for the Device.
MTU	Enter NIC MTU value. The default value is 1,500 Byte. It is recommended to check the MTU value of the gateway first and then set the device MTU value equal to or a little bit smaller than the gateway value. It is to reduce the packets and enhance network transmission efficiency.  CAUTION Changing MTU value will result in NIC reboot and network offline. It will affect the running operations. Be careful!

6) Click **OK**.

The system returns to the **IP Set** interface.

Step 3 Configure the DNS server.

You can choose to automatically obtain DNS server address or manually enter the address.



NOTE

This step is necessary when domain name service is enabled.

- **Obtain DNS server address automatically:** Select the check box and the system can automatically obtain IP address of the DNS server in the network.
- **Use the following DNS server address:** Select the check box and then enter the IP address of preferred DNS server and alternate DNS server.

Step 4 Set the default NIC.

Click the **Default Ethernet** drop-down list to select the default NIC according to practical needs.



NOTE

Only the NIC connected to the network can be set as default NIC.

Step 5 Click **Next** to save the configuration.

4.2.3 P2P

P2P is a kind of convenient private network penetration technology. You do not need to apply for dynamic domain name, doing port mapping or deploying transit server. Scan the QR code to download a cellphone APP. After registering the device on the cellphone APP, you can perform operations such as viewing remote video and playing back records.



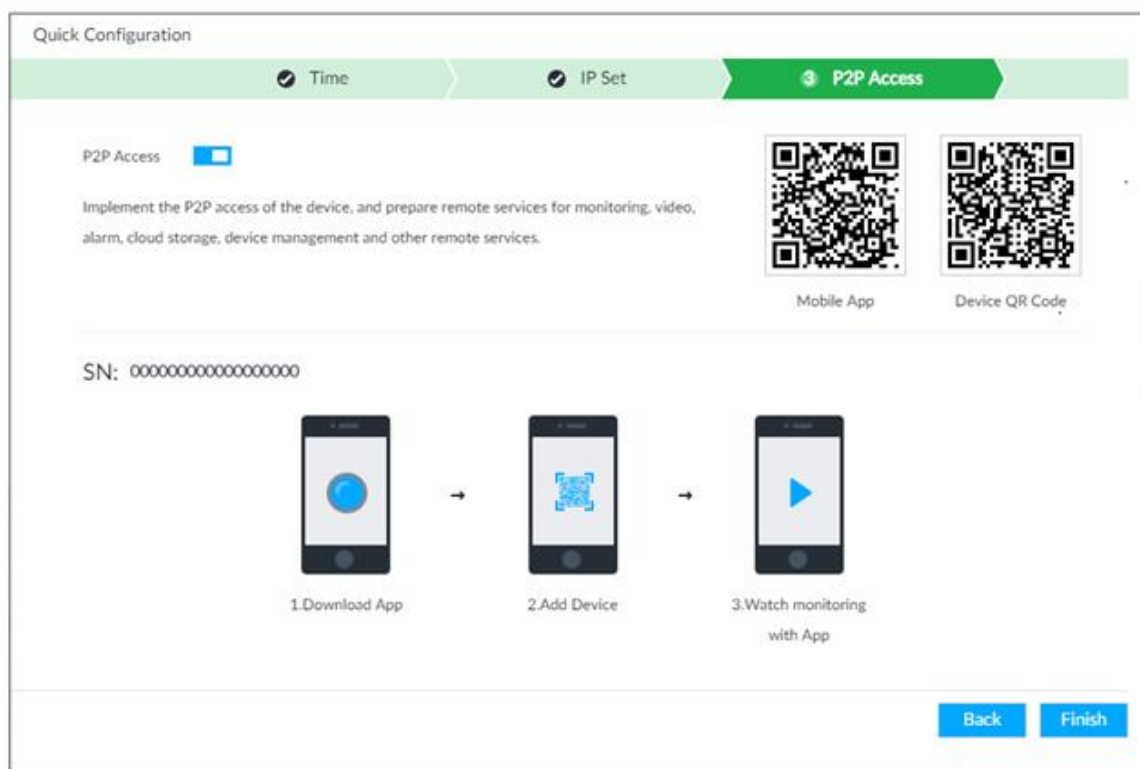
NOTE

You have to connect the Device to the external network when enabling P2P function.

Step 1 Click **Next** on the IP setting interface.

The P2P access setting interface is displayed. See Figure 4-7.

Figure 4-7 P2P access



Step 2 Click  to enable P2P access (enabled by default).

Step 3 Click **Finish** to save the configuration.

After the configuration, you can register device on the cellphone APP and view remote videos and play back records on the APP. For details, see *Cellphone APP Operations*.

Cellphone APP Operations

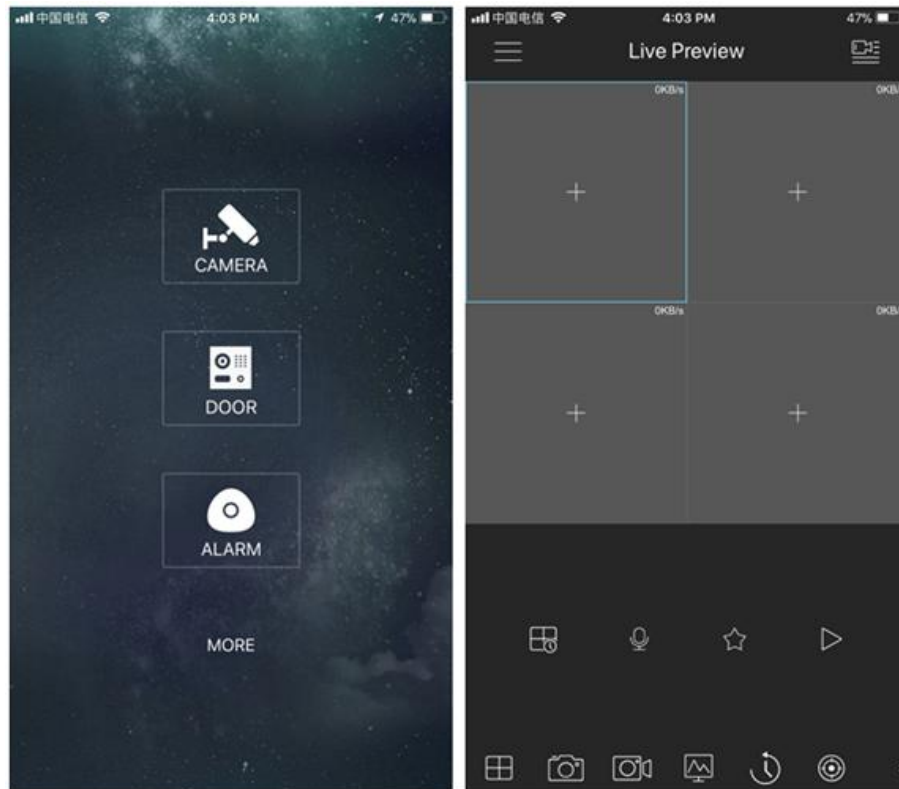
Step 1 Download and install cellphone APP.

- 1) Scan the QR code for APP download with any available application.
- 2) Download and install the APP according to the cellphone model.

Step 2 Open the APP and tab **CAMERA**.

The **Live Preview** interface is displayed. See Figure 4-8.

Figure 4-8 Cellphone APP



Step 3 Register device on cellphone APP.



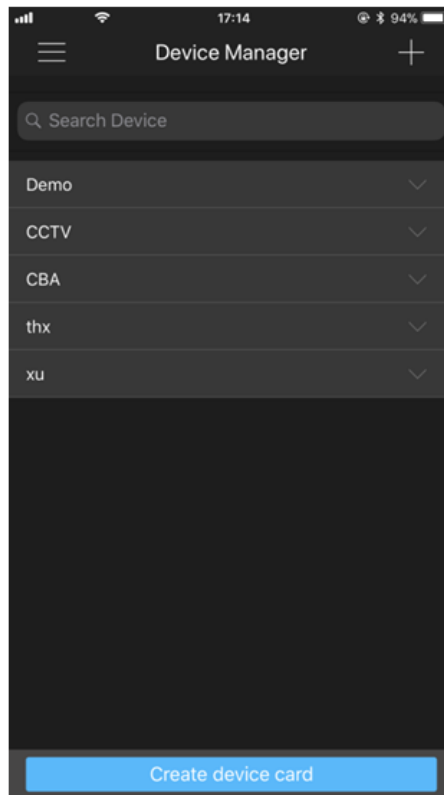
NOTE

Before registering device on the cellphone APP, make sure that the device has been initialized. Otherwise, it cannot be used normally.

- 1) Tab  and then tab **Device Manager**.

The **Device Manager** interface is displayed. See Figure 4-9.

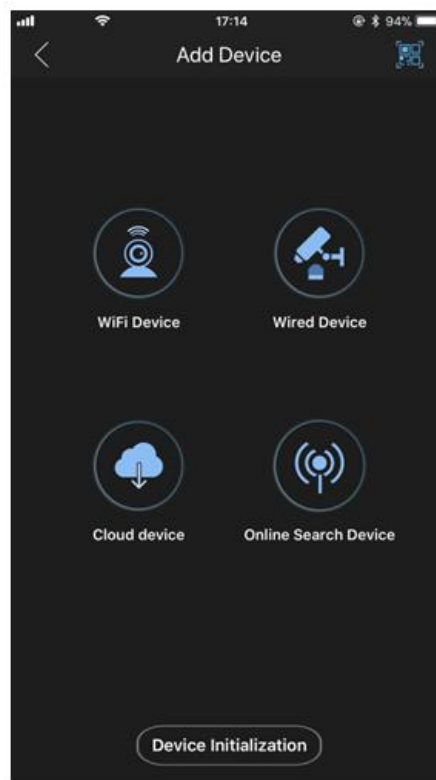
Figure 4-9 Device manager



2) Tap .

The **Add Device** interface is displayed. See Figure 4-10.

Figure 4-10 Device register



3) Select the connection type and connect the device according to the prompts. The system displays the device serial number. See Figure 4-11.

Figure 4-11 Connection information

The screenshot shows a mobile application interface for P2P connection. At the top, there's a status bar with signal, Wi-Fi, time (17:14), and battery (94%). Below is a header with a back arrow and 'P2P'. The main area contains several rows of settings: 'Register Mode' set to 'P2P', 'Name' set to 'IVSS', 'SN' set to '3B039C2YAZB5FE4', 'Username' set to 'admin', 'Password' masked with seven dots, 'Live Preview' set to 'Extra >', and 'Playback' set to 'Extra >'. At the bottom is a large blue button labeled 'Start Live Preview'.

 NOTE

You can also connect the device by scanning the QR code. The operation steps are shown as follows.

Tab  to enter the P2P interface of the actual device and scan the QR code displayed in **Device QR Code**.

- 4) Enter the device name, user name and password according to practical needs.

Step 4 Tab **Start Live Preview**.

The system starts to connect the device. After connecting successfully, the system displays the live preview interface.

4.3 IPC Settings

The section introduces the IPC initial configurations such as IPC initialization and face detection configuration.

When AI by camera is enabled, IVSS device only supports functions such as enabling AI by camera, enabling face ROI, period configuration and alarm activation. You can log in Web interface of the IPC to configure the detailed properties of face detection.

 NOTE

- You can also use the ConfigTool to initialize the IPC and modify IP address. For details, see *IPC User's Manual*.
- Before configuration, make sure the network between PC, IVSS and IPC are connected.
- IPC default IP address: 192.168.1.108. It is recommended to configure a suitable IP address according to the actual network situation.

- The following figures are for reference only. The actual interface shall prevail.

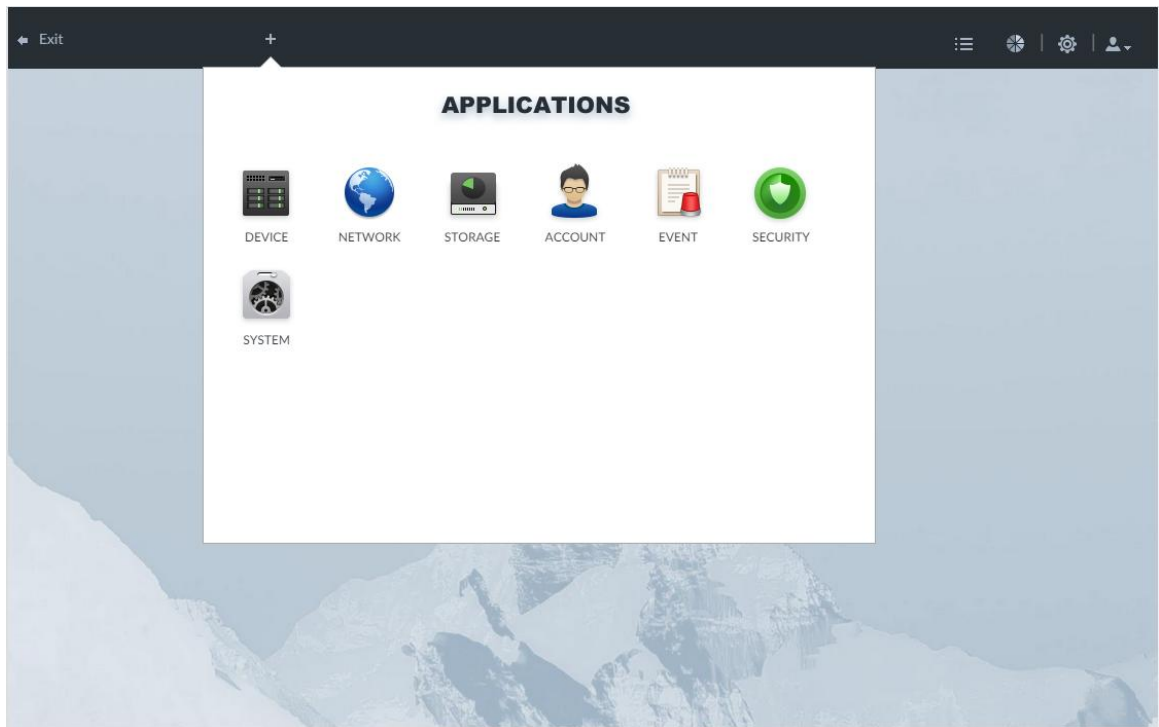
4.3.1 Initializing IPC

When you use the IPC for the first time, you need to initialize IPC first, that is to set the IPC login password and IP address.

Step 1 Click  and select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 4-12.

Figure 4-12 Device Setting



Step 2 Click  or click **Add** and select the **Smart Add** tab.

The **Smart Add** interface is displayed. See Figure 4-13.

Figure 4-13 Smart add

Add Device

Smart Add

Manual Add

▶ Start Search

Initialize

Modify IP

There are no rows in the table!

Bandwidth : 14.83Mbps/512Mbps

Add

Cancel

Step 3 Search remote device.



NOTE

If there is no specified search condition, the system searches for the remote devices in the same IP segment by default.

- 1) Click .

The **Add** interface is displayed. See Figure 4-14.

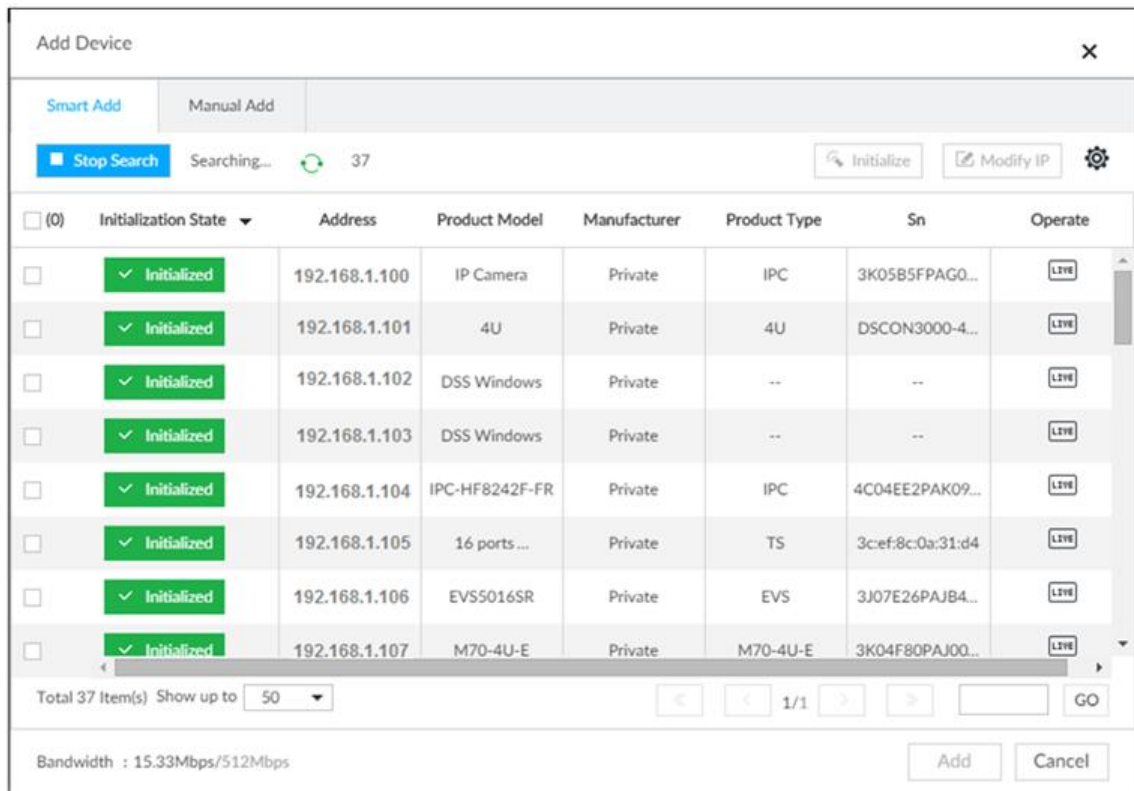
Figure 4-14 Add

- 2) Select the manufacturer and enter the IP address to search for.
 - IP address: Enter the IP address of the remote device. The system only searches for the corresponding remote device.
 - IP segment: Enter the IP segment range of the remote device. The system searches for the remote devices within the segment range.
- 3) Click **OK** to save the configuration.

The system returns to the **DEVICE** interface.
- 4) Click **Start Search**.

The system starts to search the remote devices and displays the results. See Figure 4-15.

Figure 4-15 Remote device



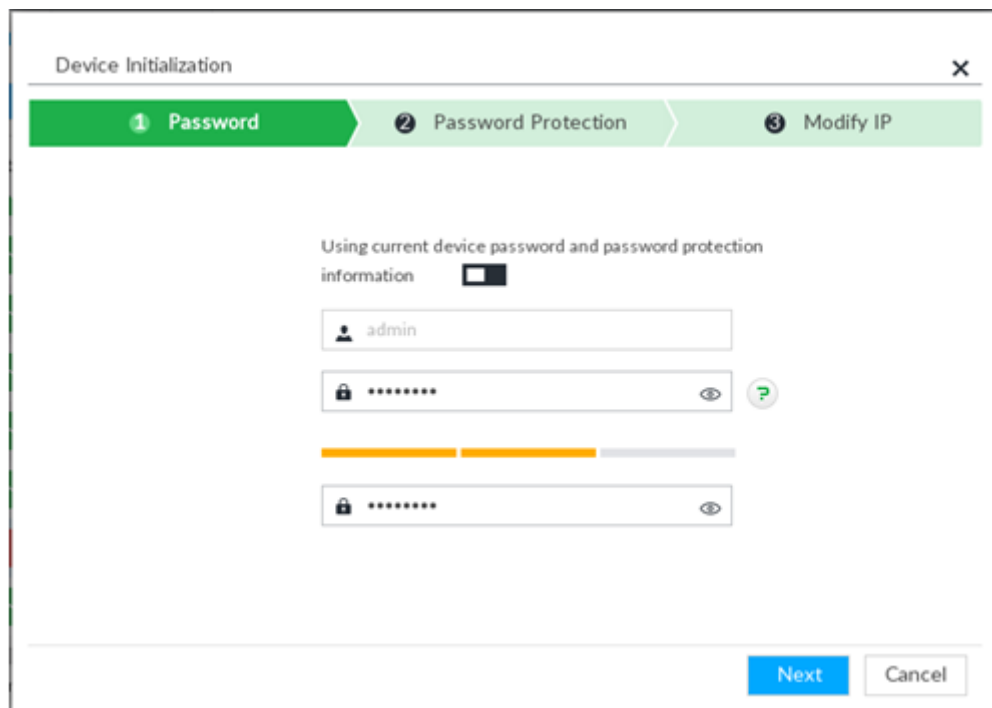
Step 4 Select the uninitialized device and click **Initialize**.

The **Device Initialization** interface is displayed. See Figure 4-16.

🔑 TIPS

Click the drop-list of **Initialization State** and select **Uninitialized** to quickly screen out the uninitialized devices.

Figure 4-16 Device initialization (1)



Step 5 Configure the remote device password and password protection.

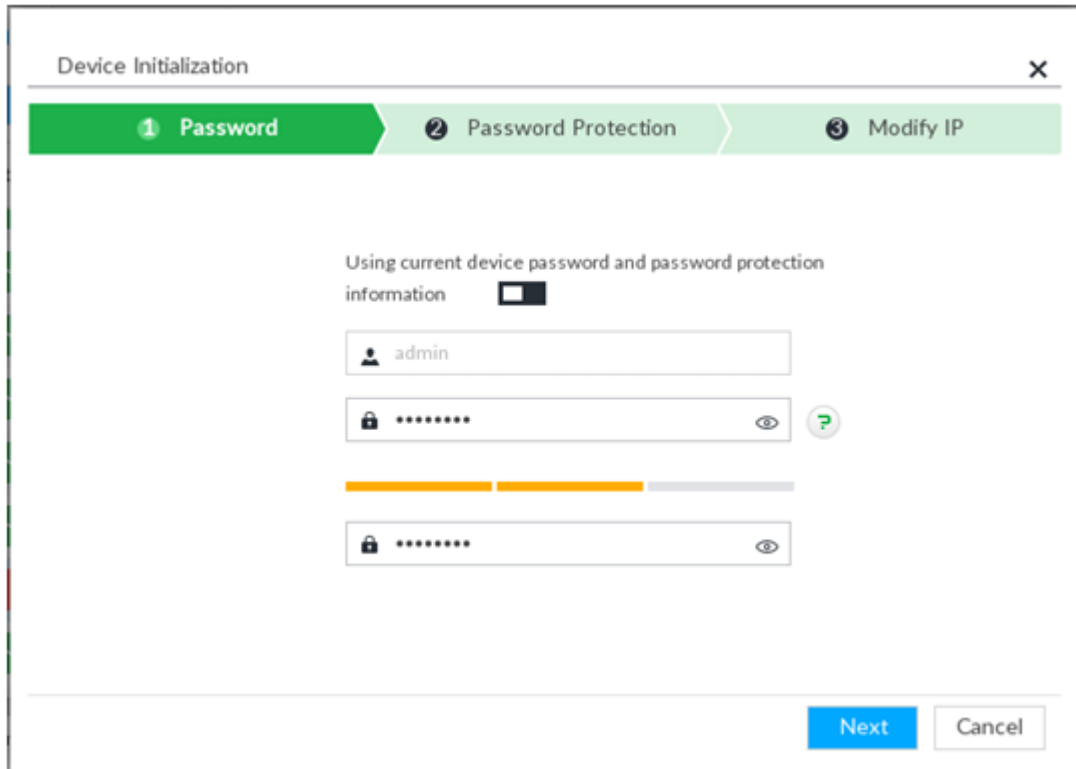
 NOTE

Using current device password and password protection information: Enable it to use current device admin account and email information. There is no need to configure password and email again. Go to Step 6.

- 1) Click .

The password setting interface is displayed. See Figure 4-17.

Figure 4-17 Device initialization (2)



- 2) Configure the parameters. For details, see Table 4-5.

Table 4-5 Description of password setting parameters

Parameter	Description
User	The default username is admin .
Password	The password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special character (excluding "", "", ";", ":" and "&"). It is recommended to set a password of high security according to the prompt.
Confirm password	 TIPS After entering the password, press and hold down  with the mouse to display the password characters. Release the mouse or move the cursor to other position, the password is displayed at hidden mode again.

- 3) Click **Next**.

The password protection setting interface is displayed. See Figure 4-18.

Figure 4-18 Password protection

The screenshot shows a 'Device Initialization' window with a progress bar at the top. The progress bar has three steps: 'Password' (completed with a checkmark), '2 Password Protection' (current step, highlighted in green), and '3 Modify IP'. Below the progress bar, the text 'Email (To reset password)' is displayed above a text input field containing the placeholder 'Email' with an envelope icon. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

4) Enter the reserved email.

You can reset the password via the reserved email in case you forgot it.

Step 6 Click **Next**.

The modifying IP address interface is displayed. See Figure 4-19.

Figure 4-19 Modifying IP

The screenshot shows the 'Device Initialization' window at the '3 Modify IP' step. The progress bar now shows 'Password' and 'Password Protection' as completed steps, and '3 Modify IP' as the current step. Below the progress bar, there is a table with two columns: '(1) Sn' and 'IP Address'. The first row contains the values '32:c5:f8:1d:f1:b1' and '192.168.1.102'. Below the table, there are radio buttons for 'DHCP' and 'Static', with 'Static' selected. Under the 'Static' option, there are input fields for 'Static IP Address', 'Subnet Mask', and 'Gateway', each containing a dot as a placeholder. To the right of these fields is an 'Incremental Value' field containing the number '1'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Step 7 Configure IP address for the IPC.

- DHCP: There is no need to enter IP address, subnet mask, and default gateway. Device automatically allocates the IP address to the camera.
- Static: Enter static IP address, subnet mask, gateway and incremental value. After you enter incremental value, system can add the fourth segment of the IP address one by one to automatically allocate the IP addresses.



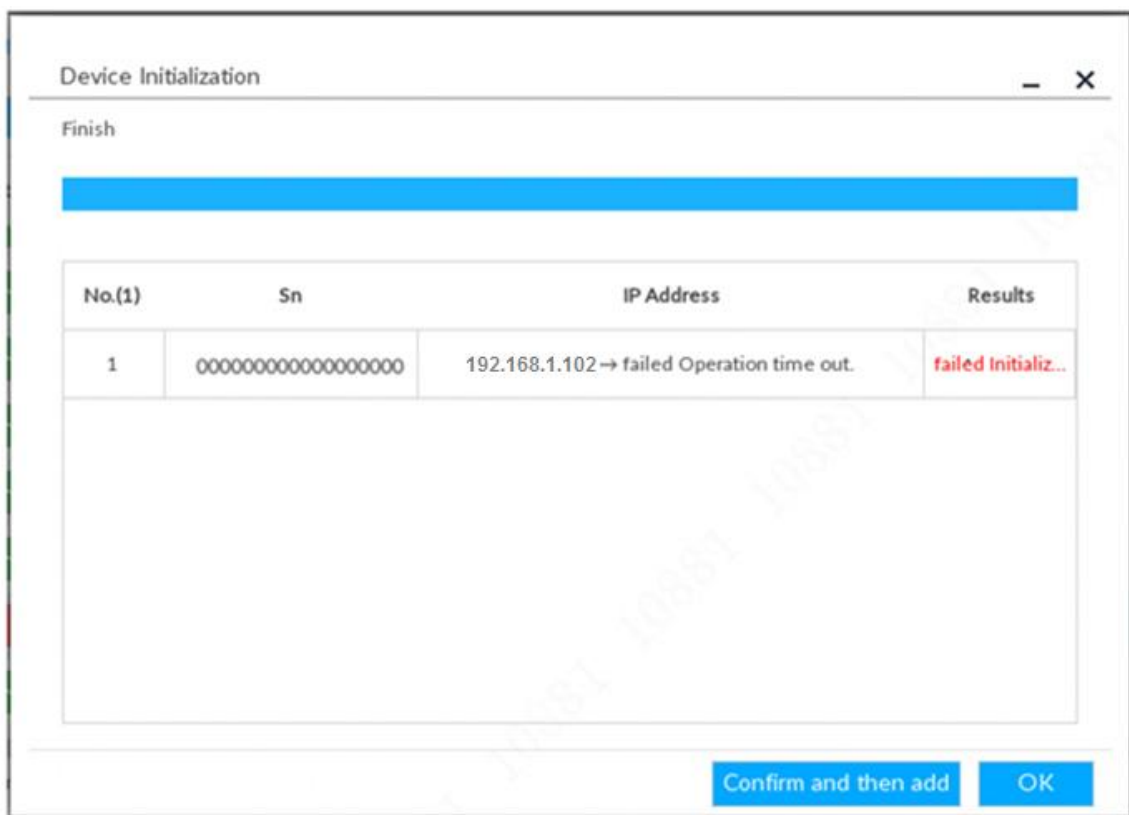
NOTE

- When you change several IP addresses at the same time, the IP addresses from different segments will be changed to the same segment.
- If there is IP conflict when changing static IP address, device pops up IP conflict dialogue box. If change IP address in batch, device automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 8 Click **Next**.

The system starts to initialize the remote device. See Figure 4-20.

Figure 4-20 Initializing results



Step 9 System completes remote device initialization.

- Click **Confirm and then add**: System completes initializing the remote device and then adds the remote device to the list. System goes back to **Add Device** interface.
- Click **OK**: System completes initializing remote device. System goes back to **Add Device** interface.

4.3.2 Enabling Human Face Detection

Enable IPC human face detection function.

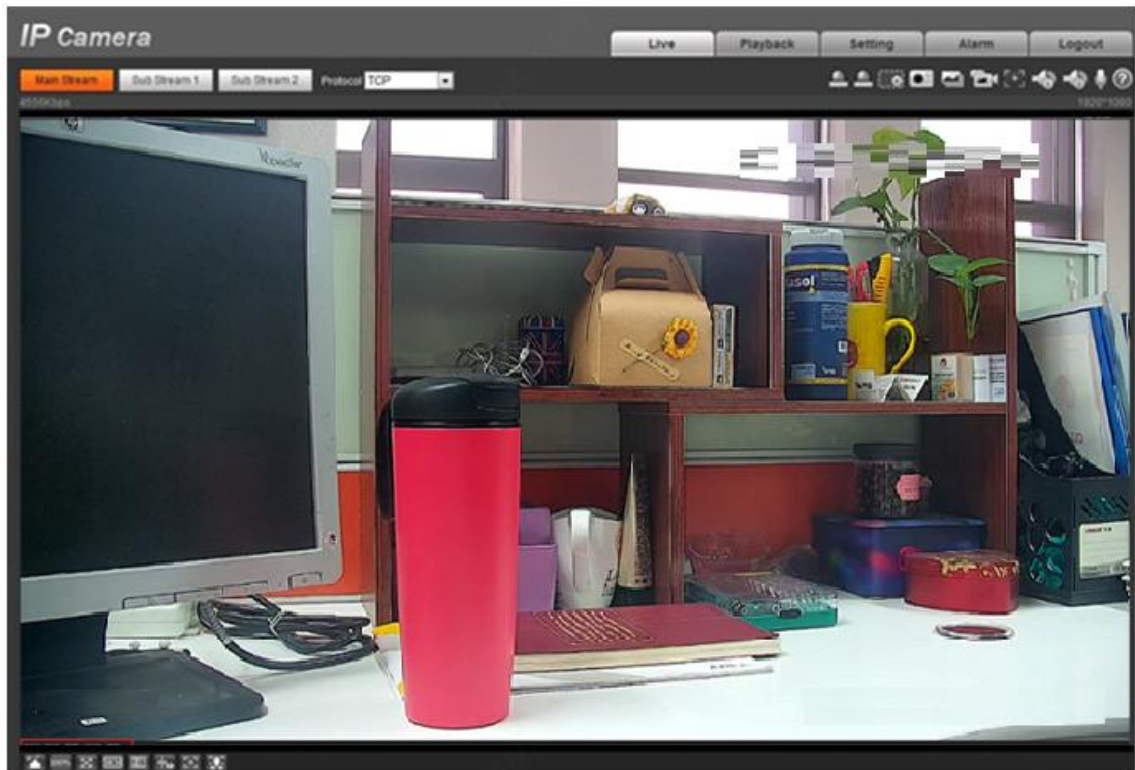
Step 1 Log in the Web interface of IPC.

- 1) Open the browser and enter the IP address of IPC. Click Enter key.
If the **Online Upgrade Wizard** is displayed, do according to the system prompt.

- 2) Enter the IPC user name and password.
- 3) Click **Log in**.

When log in the Device for the first time, click **Please click here to download the plugin** and install the control according to system prompts. After installing the control, the main interface is displayed. See Figure 4-21.

Figure 4-21 Web main interface

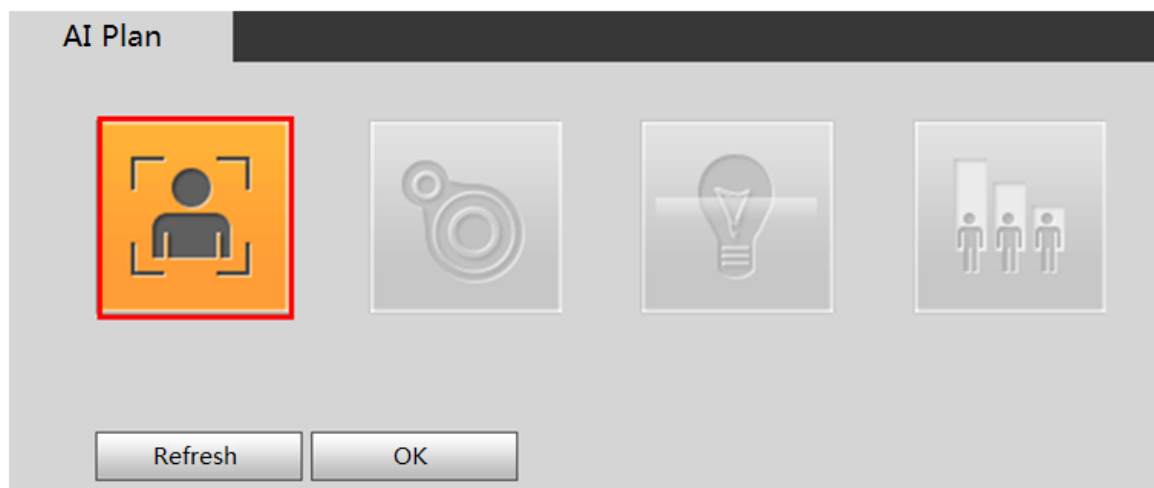


Step 2 Select **Setting > Event > AI Plan**.

The **AI Plan** interface is displayed.

Step 3 Select the AI plan for human face detection. See Figure 4-22.

Figure 4-22 AI plan of human face detection



Step 4 Click **OK** to save the configuration.

4.3.3 Configuring Human Face Detection

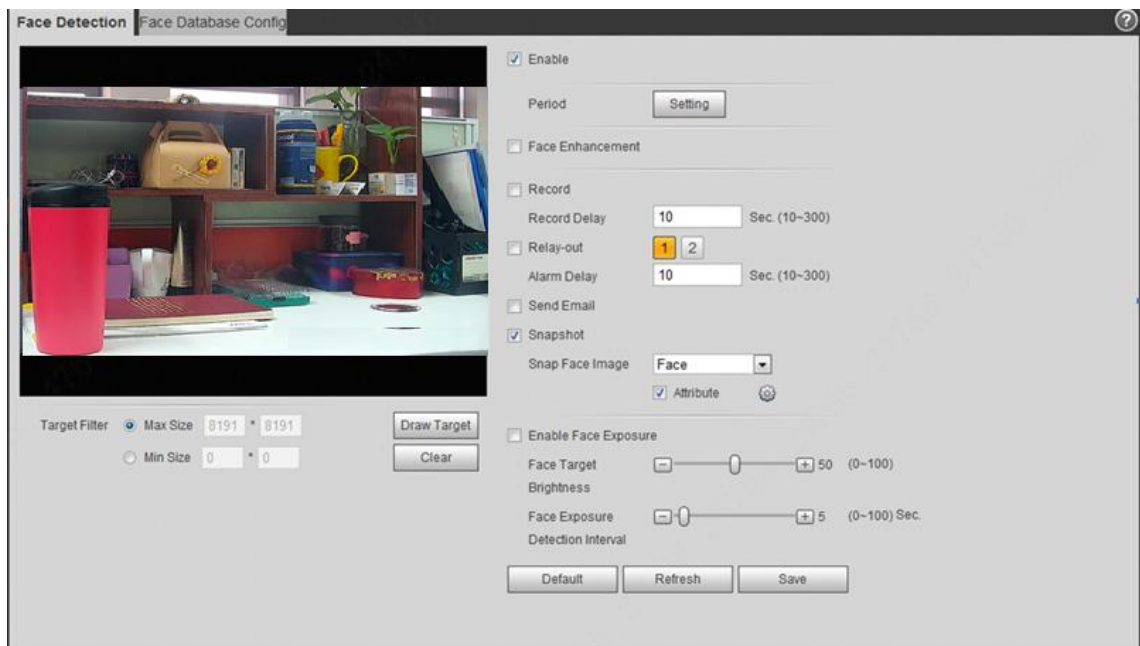
Enable IPC human face detection and configure alarm activation.

Step 1 Log in the Web interface of IPC. For details, see Step 1 of "4.3.2 Enabling Human Face Detection."

Step 2 Select **Setting > Event > Face Detect**.

The **Face Detect** interface is displayed. See Figure 4-23.

Figure 4-23 Human face detection



Step 3 Select the **Enable** check box to enable this function.

Step 4 Configure the alarm activation parameters according to practical needs. For details, see *IPC User's Manual*.

Step 5 Click **OK** to save the configuration.

4.4 Registering IPC

After you register the remote device to the system, you can view the real-time video from the remote device and change remote device settings.

Device supports two add modes: Smart add and manual add.



CAUTION

Uninitialized IPC cannot be registered to the system. For detailed operations to initialize IPC, see "4.3.1 Initializing IPC."

4.4.1 Short-Cut Menu

It is to search the remote devices in the same network and then filter to register. It is useful if you do not know the exact IP address.

Step 1 Click

The applications interface is displayed.

Step 2 Click **DEVICE**.

The **DEVICE** interface is displayed. See Figure 4-24.

Figure 4-24 Device manager

DEVICE INFO	
Type	IVSS
SN	0000000000000000
MAC1	3cef8c39:23:46
MAC2	3cef8c39:23:47
MAC3	3cef8c39:23:44
MAC4	3cef8c39:23:45
Input bandwidth	9.26Mbps/512.00Mbps
Video Out	3
Audio In/Out	1/4
Alarm In/Out	16/8
System Version	1.000.0000000.3.R, Build Date: 2018-05-11 23:13:34
WEB Version	4.0.0.97643

Step 3 Click  or click **Add** and select the **Smart Add** tab.

The **Smart Add** interface is displayed. See Figure 4-25.

Figure 4-25 Smart add

There are no rows in the table!

Bandwidth : 6.4Mbps/512Mbps

Step 4 Search remote device.

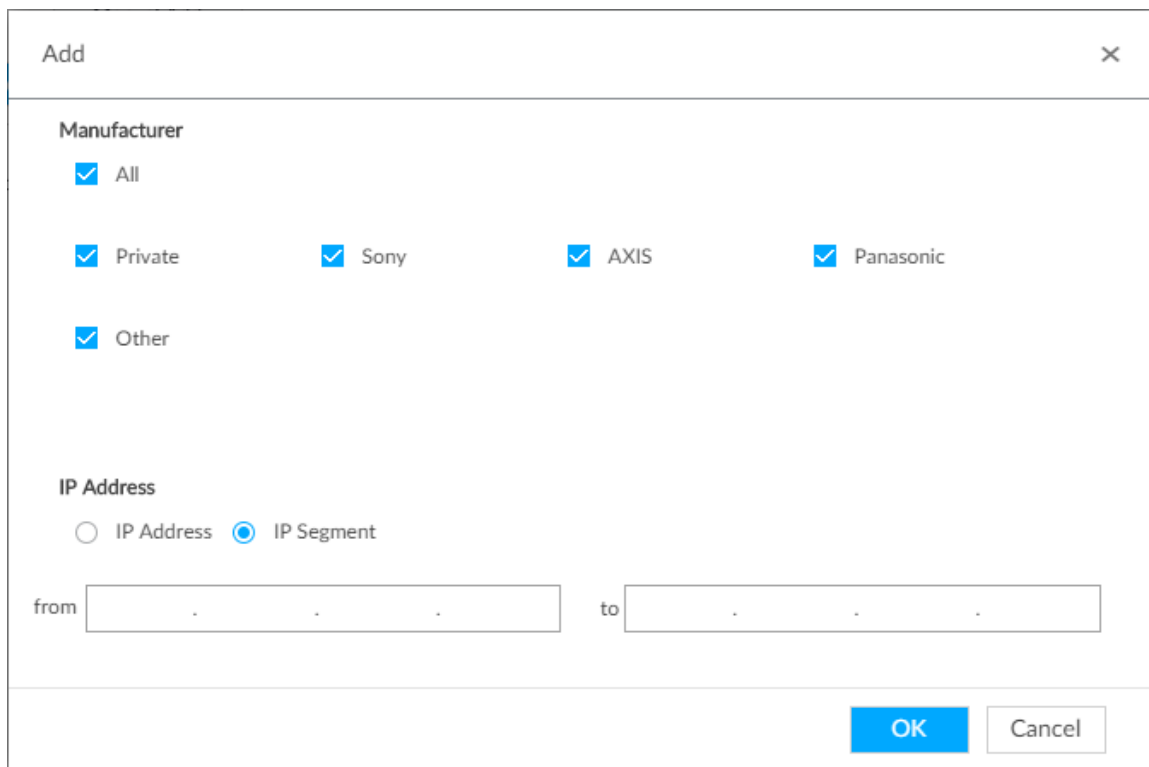
 NOTE

If there is no specified search condition, the system searches for the remote devices in the same IP segment by default.

- 1) Click .

The **Add** interface is displayed. See Figure 4-26.

Figure 4-26 Remote device register



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Manufacturer" and "IP Address".

Manufacturer Section:

- ☒ All
- ☒ Private ☒ Sony ☒ AXIS ☒ Panasonic
- ☒ Other

IP Address Section:

☐ IP Address ☒ IP Segment

from to

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white).

- 2) Select the manufacturer and enter the IP address to search for.
 - IP address: Enter the IP address of the remote device. The system only searches for the corresponding remote device.
 - IP segment: Enter the IP segment range of the remote device. The system searches for the remote devices within the segment range.
- 3) Click **OK** to save the configuration.

The system returns to the **Add Device** interface.
- 4) Click **Start Search**.

The system starts to search the remote devices and displays the results. See Figure 4-27.

Figure 4-27 Search results

Add Device							
Smart Add		Manual Add					
Stop Search		Searching...		37		Initialize	Modify IP
☐ (0)	Initialization State	Address	Product Model	Manufacturer	Product Type	Sn	Operate
☐	✓ Initialized	192.168.1.100	IP Camera	Private	IPC	3K0585FPAG0...	LIVE
☐	✓ Initialized	192.168.1.101	4U	Private	4U	DSCON3000-4...	LIVE
☐	✓ Initialized	192.168.1.102	DSS Windows	Private	--	--	LIVE
☐	✓ Initialized	192.168.1.103	DSS Windows	Private	--	--	LIVE
☐	✓ Initialized	192.168.1.104	IPC-HF8242F-FR	Private	IPC	4C04EE2PAK09...	LIVE
☐	✓ Initialized	192.168.1.105	16 ports...	Private	TS	3c:ef:8c:0a:31:d4	LIVE
☐	✓ Initialized	192.168.1.106	EVS5016SR	Private	EVS	3J07E26PAJB4...	LIVE
☐	✓ Initialized	192.168.1.107	M70-4U-E	Private	M70-4U-E	3K04F80PAJ00...	LIVE
Total 37 Item(s) Show up to 50							
Bandwidth : 15.33Mbps/512Mbps							
Add Cancel							

Step 5 Register remote device.

- Add 1-channel remote device.

Select a remote device and then click **Add**. The Device begins adding remote device and pops up confirmation interface. See Figure 4-28.



NOTE

- ◇ During the adding process, click **Cancel** to cancel adding process. Click **Stop** of the corresponding remote device to cancel the adding.
- ◇ The default username and password of remote device is admin. When it is different from the actual username and password, the adding fails.
- ◇ When the adding fails, modify information according to the prompt reason and then click **Retry** to register the remote device again.
- ◇ Double-click the remote device address, username, password, manufacturer or port to modify the corresponding information.

Figure 4-28 Add confirmation (1)

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.101	admin	*****	Private	37777	Failed to add The ...	Retry
192.168.1.102	admin	*****	Private	37777	Failed to add The ...	Retry
192.168.1.103	admin	*****	Private	37777	Added	

Bandwidth : 12.552Mbps/768Mbps

[Continue to add](#) [Finish](#)

- Add multiple-channel remote device

1) Select the remote devices and click **Add**.

The **Add Confirm** interface is displayed. See Figure 4-29.

Figure 4-29 Add confirmation (2)

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.103	admin	*****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

2) Double-click **Please select a channel** and select the channel you need to add.

3) Click **OK** to add the selected channel.

Step 6 Click **Continue to add** or **Finish**.

- Continue to add: System goes back to Smart Add interface to add more remote devices.
- Finish: Complete adding remote device. System displays Device Manager interface to view the newly added remote device information.

4.4.2 Manual Adding

To add a few remote devices, you can enter IP address, user name and password to register manually.

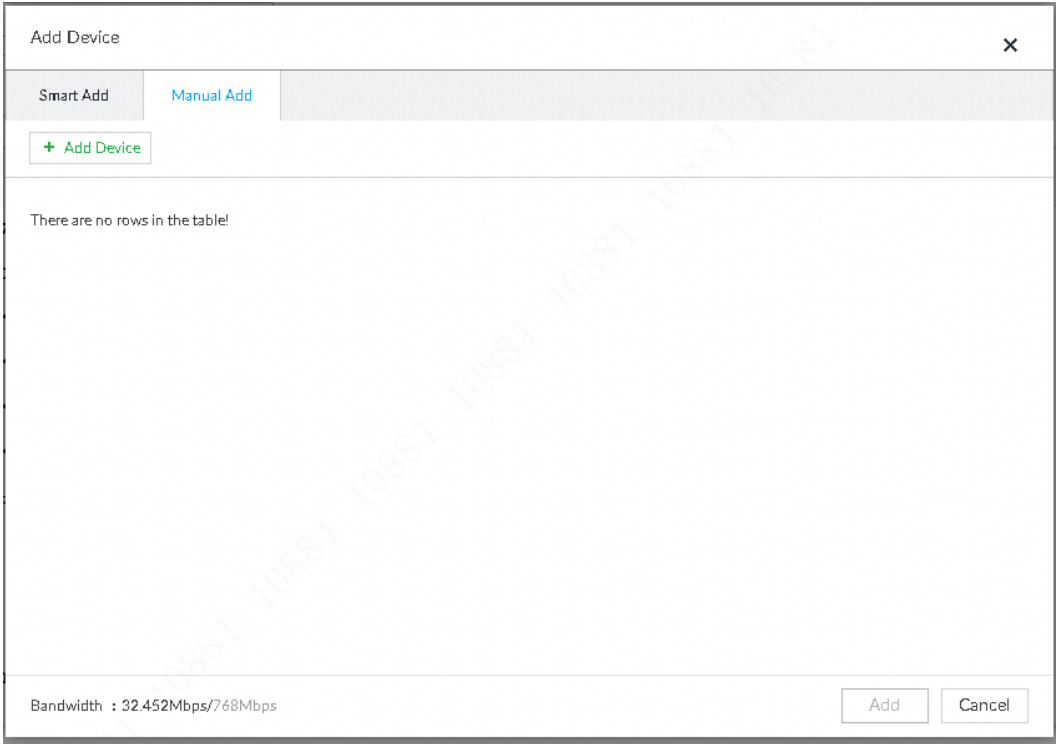
Step 1 Click  on the setting interface or click  and select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Click  or click **Add** and select the **Manual Add** tab.

The Manual Add interface is displayed. See Figure 4-30.

Figure 4-30 Manual add (1)



Add Device

Smart Add Manual Add

+ Add Device

There are no rows in the table!

Bandwidth : 32.452Mbps/768Mbps

Add Cancel

Step 3 Click **Add Device**.

System displays the remote device information you need to enter. See Figure 4-31.

Figure 4-31 Manual add (2)

The screenshot shows a web interface for adding devices. The 'Manual Add' tab is active. A table lists the added device with the following details:

Device Type	Manufacturer	Address	Username	Password	Port	Operate
Devices	Private		admin	*****	37777	[Trash Icon] [Add Icon]

At the bottom of the window, there are navigation controls showing 'Total 1 Item(s)' and 'Show up to 50'. There are also 'Add' and 'Cancel' buttons.

Step 4 Configure the parameters. For details, see Table 4-6.

Table 4-6 Description of remote device parameters

Name	Function
Device Type	It is to select remote device type. The default type is Devices .
Manufacturer	Select remote device connection protocol.
Address	Enter remote device IP address.
Username	Enter remote device username and password.
Password	
Port	Enter port number.
Operate	Delete the current line or add a new line. - Click  to delete current line information. - Click  to add a new line. Enter remote device information to add several devices at the same time.

Step 5 Add remote device.

- Add 1-channel remote device.
Select the remote device and click **Add**. Device begins to add remote device and pops up confirmation interface. See Figure 4-32.

 NOTE

- ◇ During the adding process, click **Cancel** to cancel adding process. Click **Stop** of the corresponding remote device to cancel the adding.
- ◇ When the adding fails, modify information according to the prompt reason and then click **Retry** to register the remote device again.
- ◇ Double-click the remote device address, username, password, manufacturer or port to modify the corresponding information.

Figure 4-32 Add confirmation (1)

The screenshot shows a window titled "Add Confirm" with a close button (X). Inside, there is a table with the following columns: Address, Username, Password, Manufacturer, Port, Status, and Operate. The first row contains the values: 192.168.1.105, admin, ***** (masked), Private, 40009, Please select a cha..., and an empty Operate cell. Below the table is a large empty rectangular area. At the bottom left, it says "Bandwidth : 30.949Mbps/768Mbps". At the bottom right, there are two buttons: "Continue to add" (highlighted in blue) and "Finish".

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.105	admin	*****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- Add multiple-channel remote device

1) Click **Add**.

The **Add Confirm** interface is displayed. See Figure 4-33.

Figure 4-33 Add confirmation (2)

This screenshot is identical to the one in Figure 4-32, showing the "Add Confirm" dialog box with the same table, bandwidth information, and buttons.

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.106	admin	*****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

2) Double-click **Please select a channel** and select the channel you need to add.

The Video Device interface is displayed.

3) Click **OK** to add the selected channel.

Step 6 Click **Continue to add** or **Finish**.

- Continue to add: System goes back to Manual Add interface to add more remote devices.
- Finish: Complete adding remote device. System displays Device Manager interface to view the newly added remote device information.

5

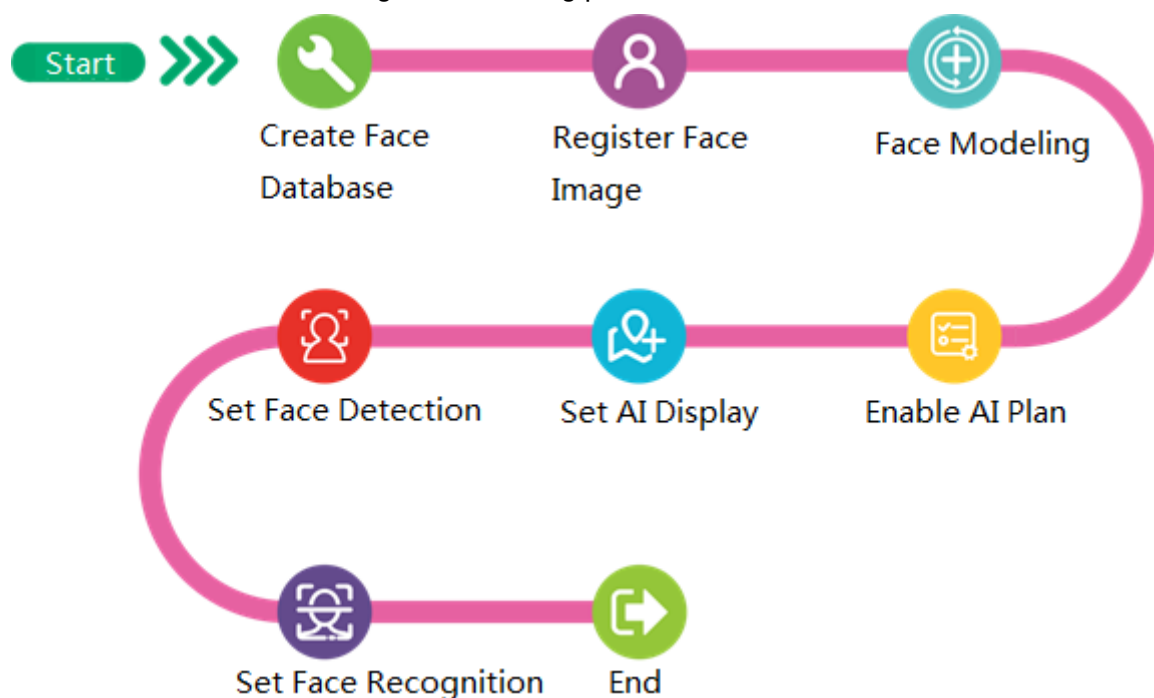
Face Recognition Arming

This section introduces the operations of human face recognition arming.

5.1 Procedure

The overall procedure of human face recognition arming is shown as in Figure 5-1.

Figure 5-1 Arming procedure



5.2 Configuring Human Face Database

After setting human face database, the intelligent detection function can trigger the human face database to compare human face, search human face and so on. The face database setting includes creating face database, adding face image and creating face module.

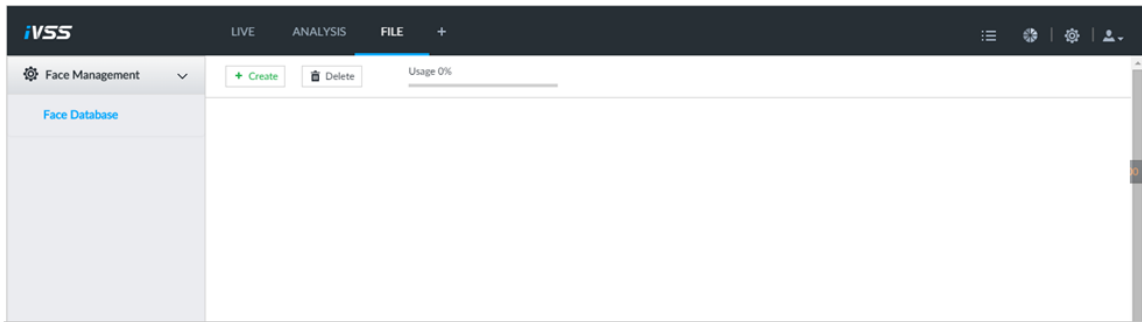
5.2.1 Creating Human Face Database

Create human face database to categorize and manage the images uploaded to the Device.

Step 1 Click  on the **LIVE** interface and select **FILE > Face Management**.

The **Face Management** interface is displayed. See Figure 5-2.

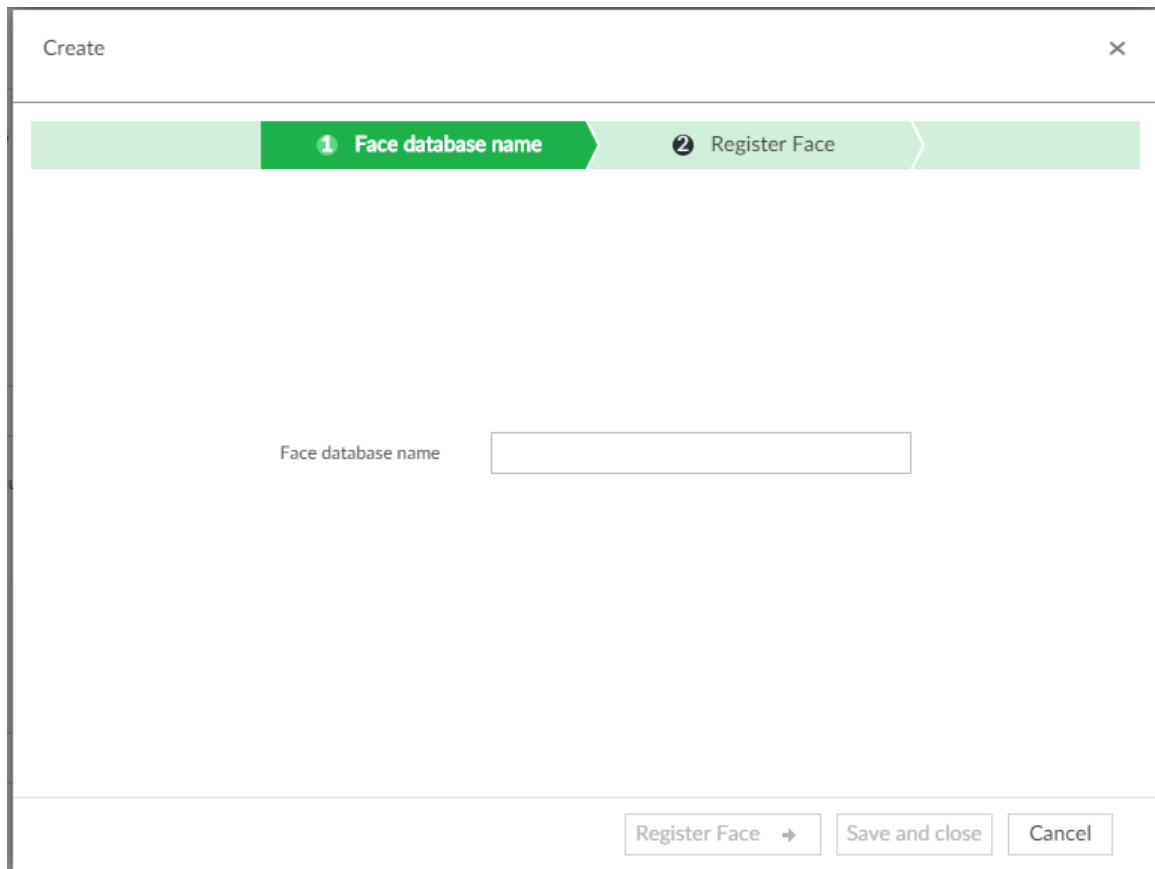
Figure 5-2 Face database management (1)



Step 2 Click .

The **Create** interface is displayed. See Figure 5-3.

Figure 5-3 Creating face database



Step 3 In the **Face database name** box, enter the database name.

Step 4 Click **Register Face** or **Save and close**.

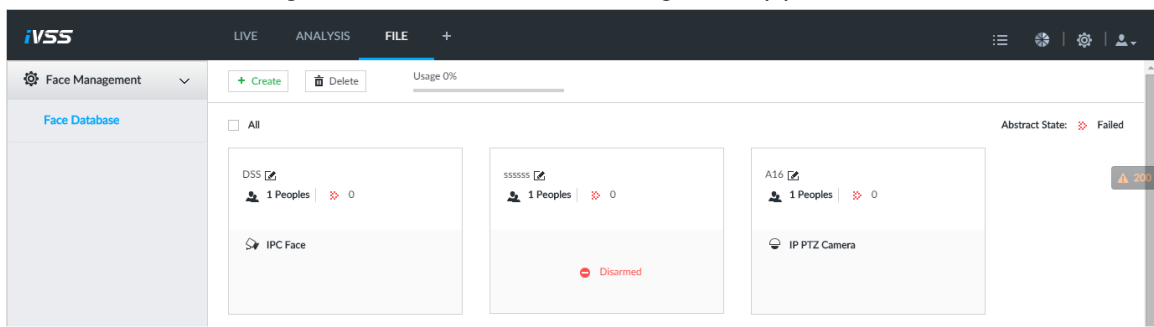
- Click **Register Face** and register face images to the created face database. See Figure 5-4. For details, see "5.2.2 Adding Human Face Image."

Figure 5-4 Face register

- Click **Save and close** to create an empty face database.

After creating the face database, you can view the database information on the **Face Management** interface. See Figure 5-5.

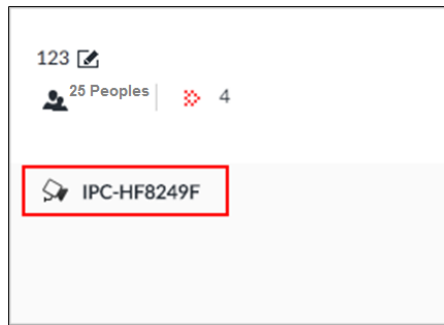
Figure 5-5 Face database management (2)



NOTE

- Click to modify the database name.
- **1 Peoples** : It displays the number of face images in the database.
- **0** : It displays the failed number of face module creation. For details to creating face module, see "5.2.3 Human Face Modeling."
- **Disarmed** : It means the database is not linked to any channel for human face recognition. For details to enable the arming, see "5.6 Face Recognition Settings." After it is armed, system displays the linked channel number of the remote device. See Figure 5-6.

Figure 5-6 Arming



5.2.2 Adding Human Face Image

It is to add face images to the created face database. It supports manual add and batch import.

NOTE

The added face image shall meet the following criteria:

- The image format is .jpg.
- The image size shall be less than or equal to 256 KB.
- The resolution ranges from 200×200 to 6000×5000.

Preparations

- Before the operation, make sure you have created the human face database. For details, see "5.2.1 Creating Human Face ."
- Face image is saved in the USB device and you have connected the USB storage device to the Device.

NOTE

The operation is for local menu only.

5.2.2.1 Manual Add

Add human face image one by one. If there is a small number of images to register, you can adopt the manual add.

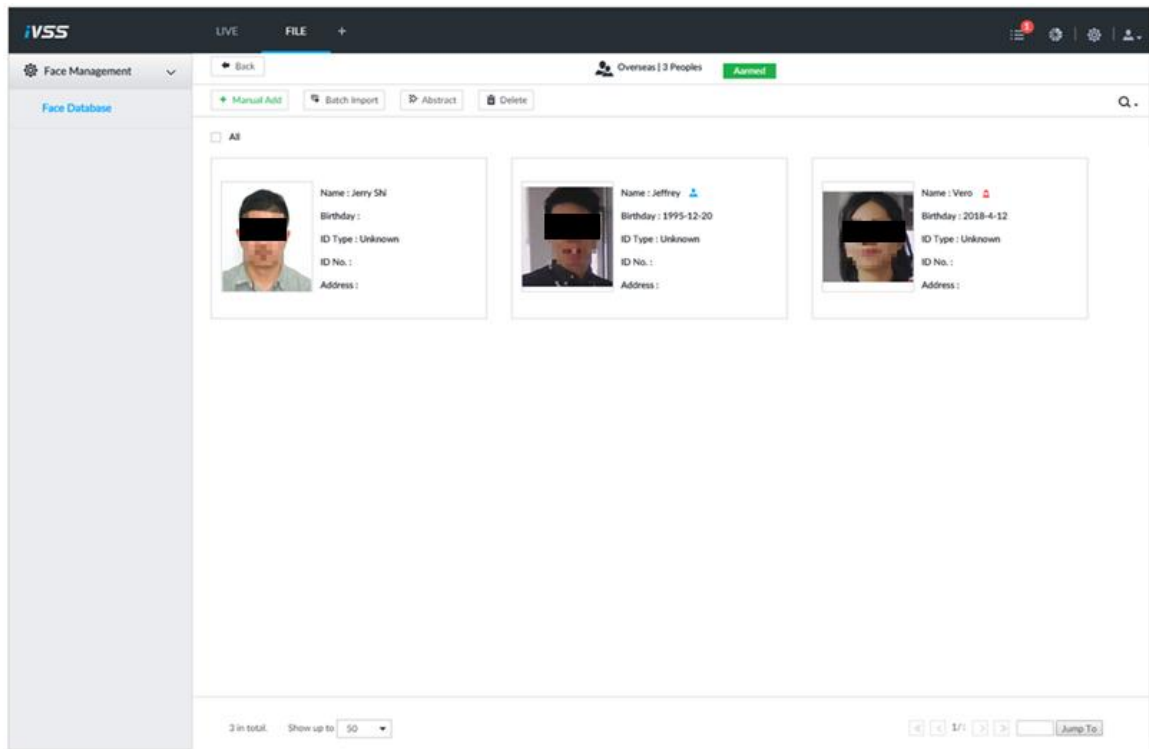
Step 1 Click  on the **LIVE** interface and select **FILE > Face Management**.

The **Face Management** interface is displayed.

Step 2 Double-click the face database.

The corresponding face database is displayed. See Figure 5-7.

Figure 5-7 Face database



Step 3 Click **Manual Add**.

The **Face Register** interface is displayed. See Figure 5-8.

Figure 5-8 Face register

The screenshot shows the 'Face Register' form. On the left is a large dashed box for a face image, with a small icon of a face with a plus sign at the bottom center. To the right of the image box are several input fields: 'Name' (text box), 'Gender' (radio buttons for 'Male' and 'Female'), 'Birthday' (text box with a calendar icon), 'Country' (dropdown menu), 'Address' (text box), 'ID Type' (dropdown menu), and 'ID No.' (text box). At the bottom right are three buttons: 'Save and continue to add', 'OK', and 'Cancel'.

Step 4 Click  to import face images.

After imported, system displays the face image in the picture frame on the left. See Figure 5-9.

- Click **Change Image** to replace the current image.
- Click  to adjust the size of the face frame.

Figure 5-9 Face image



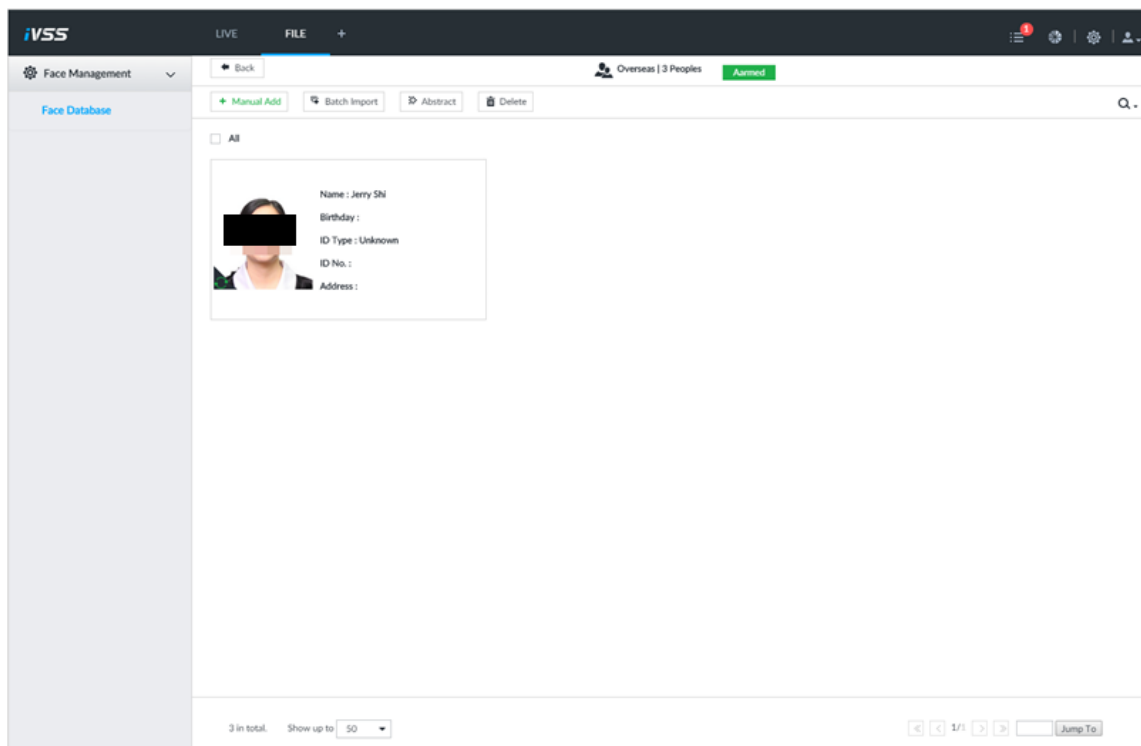
Step 5 Enter the relevant information of the current face image according to practical situation.

Step 6 Complete the face register.

- Click **Save and continue to add** to save the current face information and go on to register the next image.
- Click **OK** to save the current face information and complete the face register.

After registered,  is displayed on the lower-left corner of the image which means creating module. See Figure 5-10. For details to create face module, see "5.2.3 Human Face Modeling."

Figure 5-10 Face database (2)



5.2.2.2 Batch Add

Batch import is to import multiple face images at the same time. If you want to register a large number of face images, batch import is recommended.

Background

Before the batch import, name the face image according to the following rule:

“Name#SGender#B#Birthday#CCountry#P#Province#TID type#MID number#AAddress.jpg”
(such as “Tim#S1#B20000101#NCN#PZheJiang#T1#M0000#AAddress”).

NOTE

Name is required and the rest are optional. For example, if you want to enter the name and ID number only, the naming can be Tim#S#B#N#P#T#M0000#A.jpg or Tim#M0000.jpg.

Table 5-1 Naming rules for batch import

Item	Description
Name	Enter the corresponding name.
Gender	Enter number. 1: Male; 2: Female.
Birthday	Enter number in the format of yyyy-mm-dd. For example: 2017-11-23.
Country	Enter the corresponding country abbreviation. For details, see Table 5-2.
Province	Enter the corresponding spelling or English name of the province.
ID type	Enter the corresponding number. 1: ID card; 2: Certificate of officer; 3: Passport.
Address	Enter the detailed address.

Table 5-2 Abbreviation of countries/regions

Country	Abbreviation	Country	Abbreviation	Country	Abbreviation
China	CN	Cambodia	KH	India	IN
Malaysia	MY	Maldives	MV	Mongolia	MN
Philippines	PH	Qatar	QA	Saudi Arabia	SA
Singapore	SG	Korean	KR	Sri Lanka	LK
Turkey	TR	Thailand	TH	United Arab Emirates	AE
Vietnam	VN	Austria	AT	Belarus	BY
Belgium	BE	Bulgarian	BG	Denmark	DK
Estonia	EE	Finland	FI	France	FR
Greek	GR	Hungary	HU	Ireland	IE
Italy	IT	Lithuania	LT	Luxembourg	LU
Netherland	NL	Norway	NO	Poland	PL
Portugal	PT	Romania	RO	Russian	RU
Serbia	RS	Spain	ES	Sweden	SE
Ukraine	UA	Great Britain	GB	Argentina	AR
Bahamas	BS	Belize	BZ	Brazil	BR
Canada	CA	Chile	CL	Columbia	CO
Mexico	MX	Panama	PA	Peru	PE
American	US	Venezuela	VE	British Virgin Islands	VG
Egypt	EG	Morocco	MA	Nigeria	NG
Seychelles	SC	South Africa	ZA	Tunisia	TN

Country	Abbreviation	Country	Abbreviation	Country	Abbreviation
Australia	AU	New Zealand	NZ	Switzerland	CH
Hongkong (China)	HK	Macao (China)	MO	Taiwan (China)	TW

Step 1 Click  on the **LIVE** interface and select **FILE > Face Management**.

The **Face Management** interface is displayed.

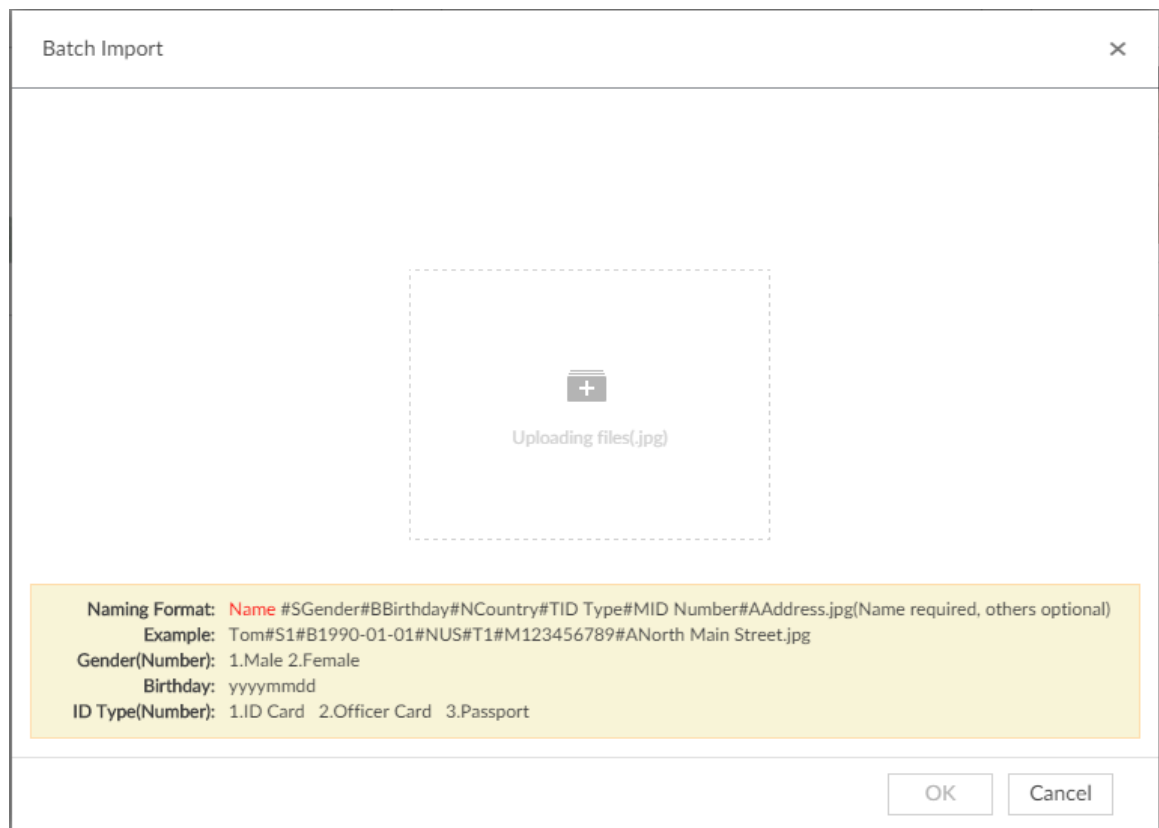
Step 2 Double-click the face database.

System displays the current face database.

Step 3 Click **Batch Import**.

The Batch Import interface is displayed. See Figure 5-11.

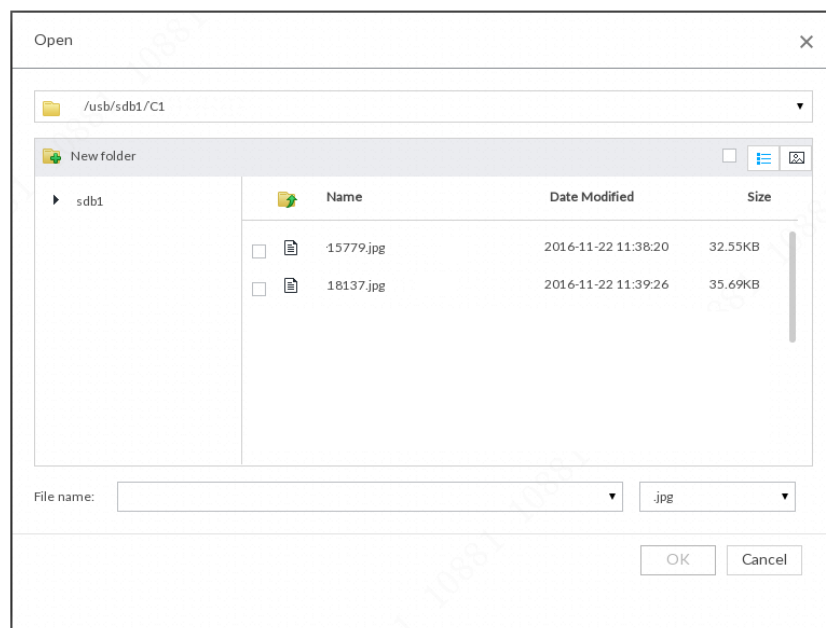
Figure 5-11 Batch import



Step 4 Click .

The **Open** interface is displayed. See Figure 5-12.

Figure 5-12 Open



Step 5 Select several face images and click **OK**.

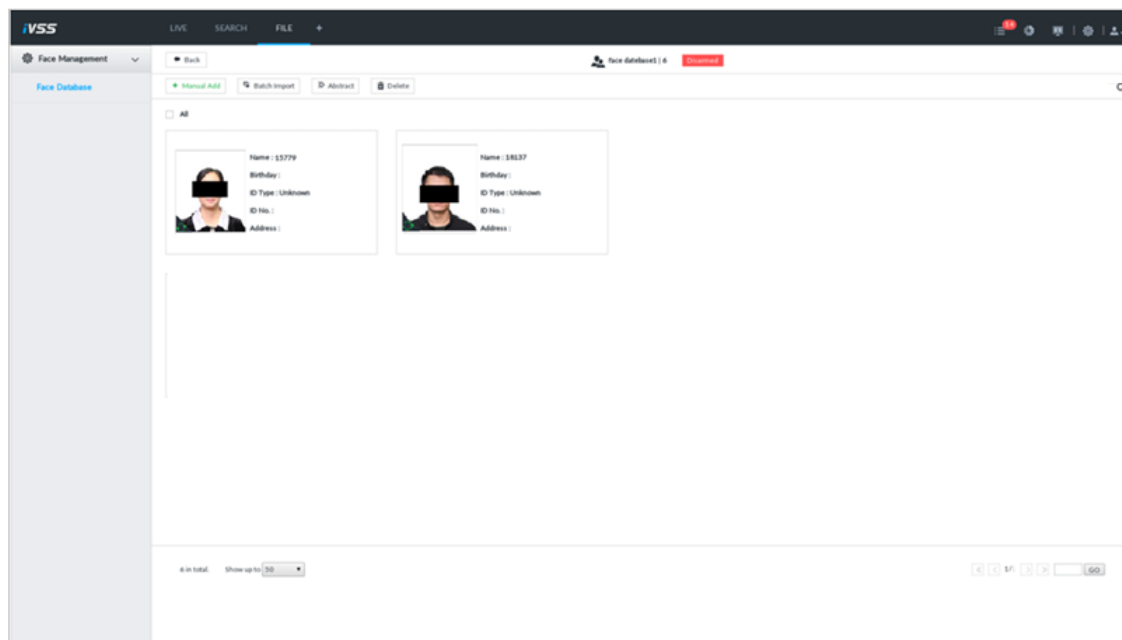
After registered,  is displayed on the lower-left corner of the image which means creating module. See Figure 5-13. For details to create face module, see "5.2.3 Human Face Modeling."



NOTE

Select one image, press and hold down the Shift key, and then click another image. You can select the two images and the other images between them.

Figure 5-13 Face database



5.2.2.3 Detection Add

On the **LIVE** interface, you can add the snapped face images to the face database directly.

Step 1 Click  on the **LIVE** interface.

The system displays the detected face images.

Step 2 Move the mouse to the image.

The icon  is displayed on the lower-left corner. See Figure 5-14.

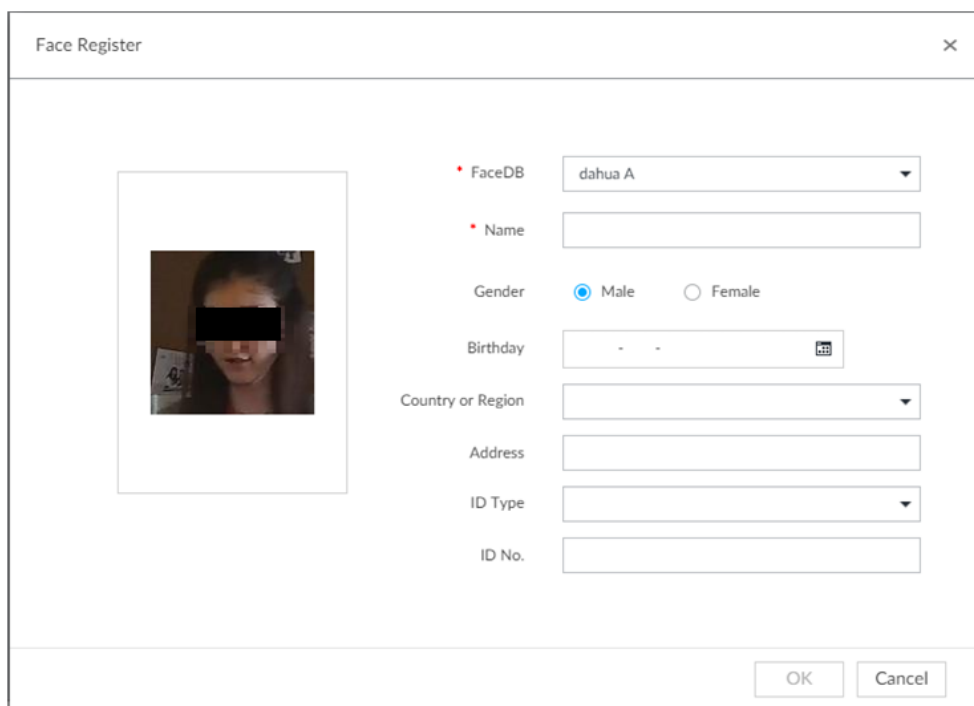
Figure 5-14 Face detection



Step 3 Click .

The **Face Register** interface is displayed. See Figure 5-15.

Figure 5-15 Face register



Step 4 In the **FaceDB** drop-down list, select the face database.

Step 5 Click OK to save the configuration.

5.2.3 Human Face Modeling

Human face modeling is to abstract the corresponding information of human face images and import it to the database to create face feature modules. The system can use them to do smart detections such as face search and face recognition.

NOTE

- The more the images, the longer it takes to create the face module. Please be patient.

- During the modeling process, some intelligent functions (such as face recognition and face search) are not available. These functions become normal after the modeling process is completed.

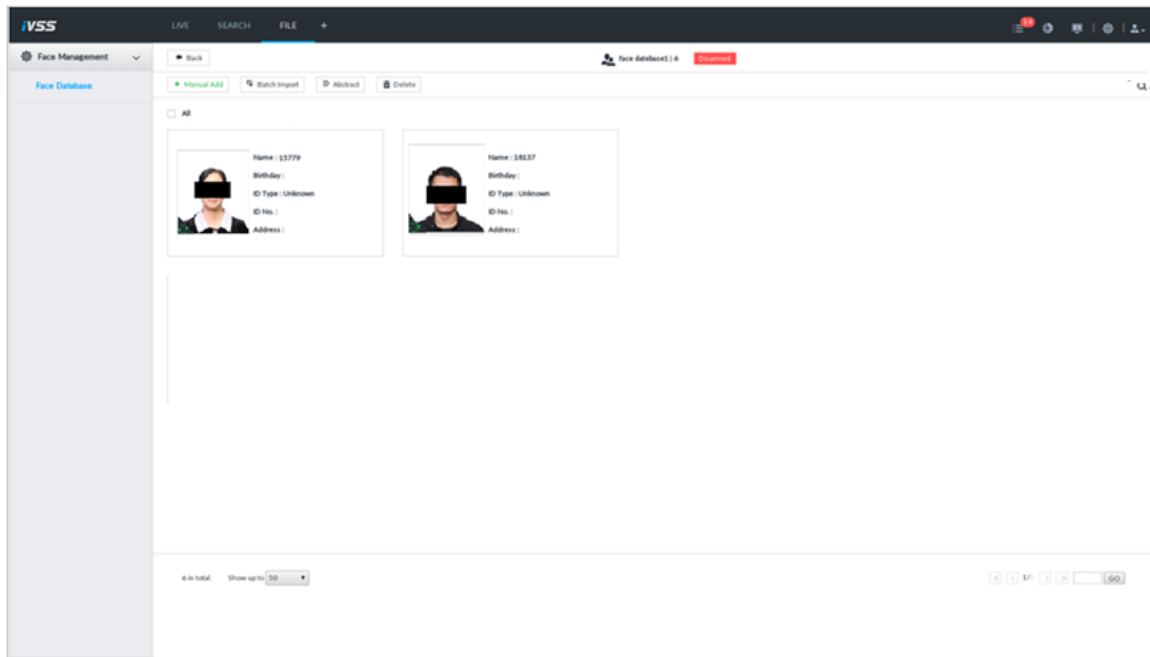
Step 1 Click  on the **LIVE** interface and select **FILE > Face Management**.

The **Face Management** interface is displayed.

Step 2 Double-click the face database.

The corresponding face database is displayed. See

Figure 5-16 Face database (1)



Step 3 Select the face image and click **Abstract**.

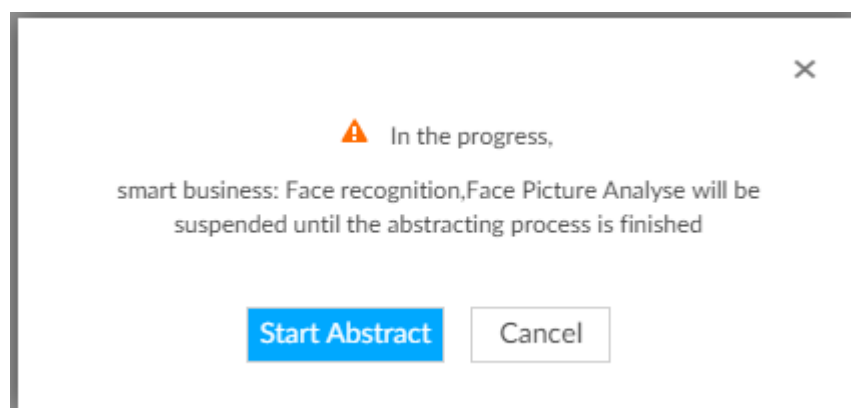
A prompt is displayed. See Figure 5-17.



NOTE

- Click **All** to select all the images in the face database.
- If there are too many face images in the face database, click  to set search criteria (such as name, gender, birthday, country and modeling status) to quickly find the face images.

Figure 5-17 Prompt

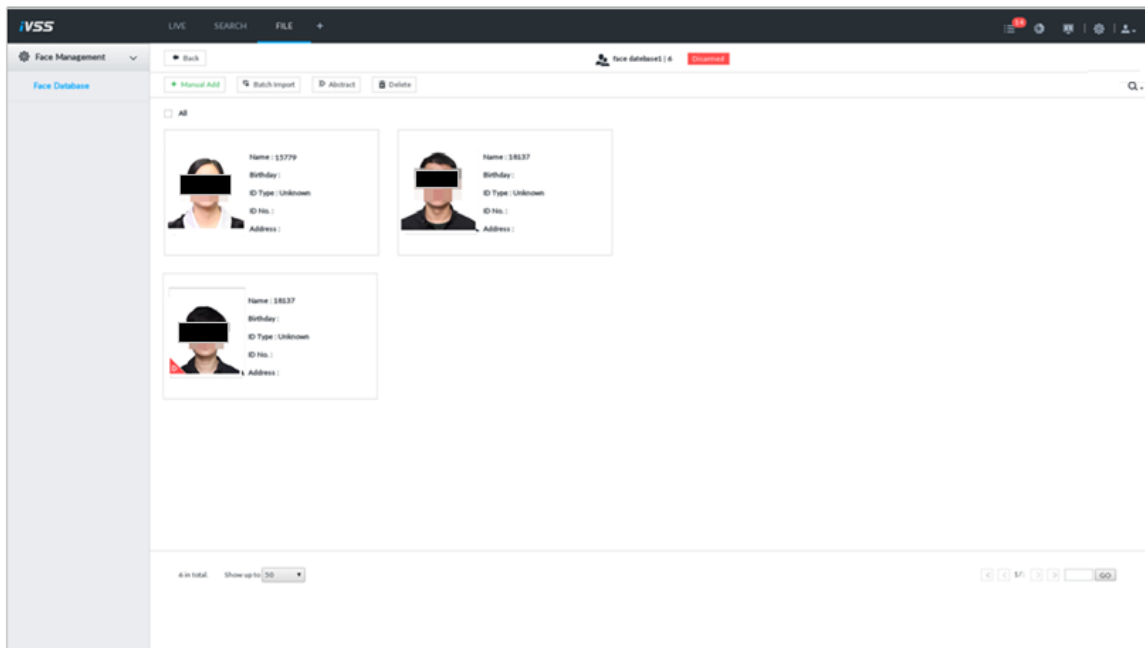


Step 4 Click Start Abstract.

The system starts to create the model. After modeling is completed, the system displays the interface shown in Figure 5-18.

- After successfully created the model, the icon  will disappear at the bottom left corner of the face image.
- The modeling might fail if the face image is not clear or does not contain complete information. The icon  is displayed at the bottom left corner of the face image.

Figure 5-18 Face database (2)



5.3 Enabling AI Plan

The AI detection function becomes valid once you enabled AI plan.

NOTE

- Some remote devices do not support AI plan. See the actual interface.
- The interface might vary since the remote device supports different AI functions. See the actual interface.

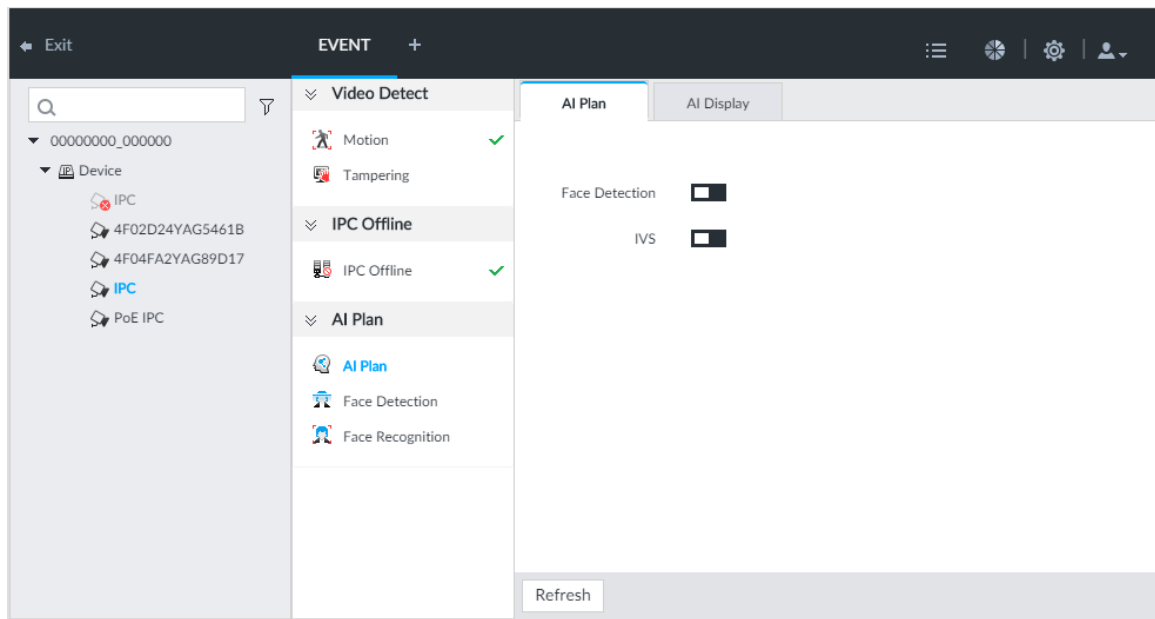
Step 1 Click  and select **EVENT**.

The **EVENT** interface is displayed.

Step 2 After selecting the remote device, select **AI Plan > AI Plan > AI Plan**.

The **AI Plan** interface is displayed. See Figure 5-19.

Figure 5-19 AI plan



Step 3 Click  to enable the corresponding AI plan.

Step 4 Click **Save** to save the configuration.

5.4 AI Display Settings

It is to set the features you want to view on the rule column and features pane. Go to the rule column and feature pane to view the AI detect results.

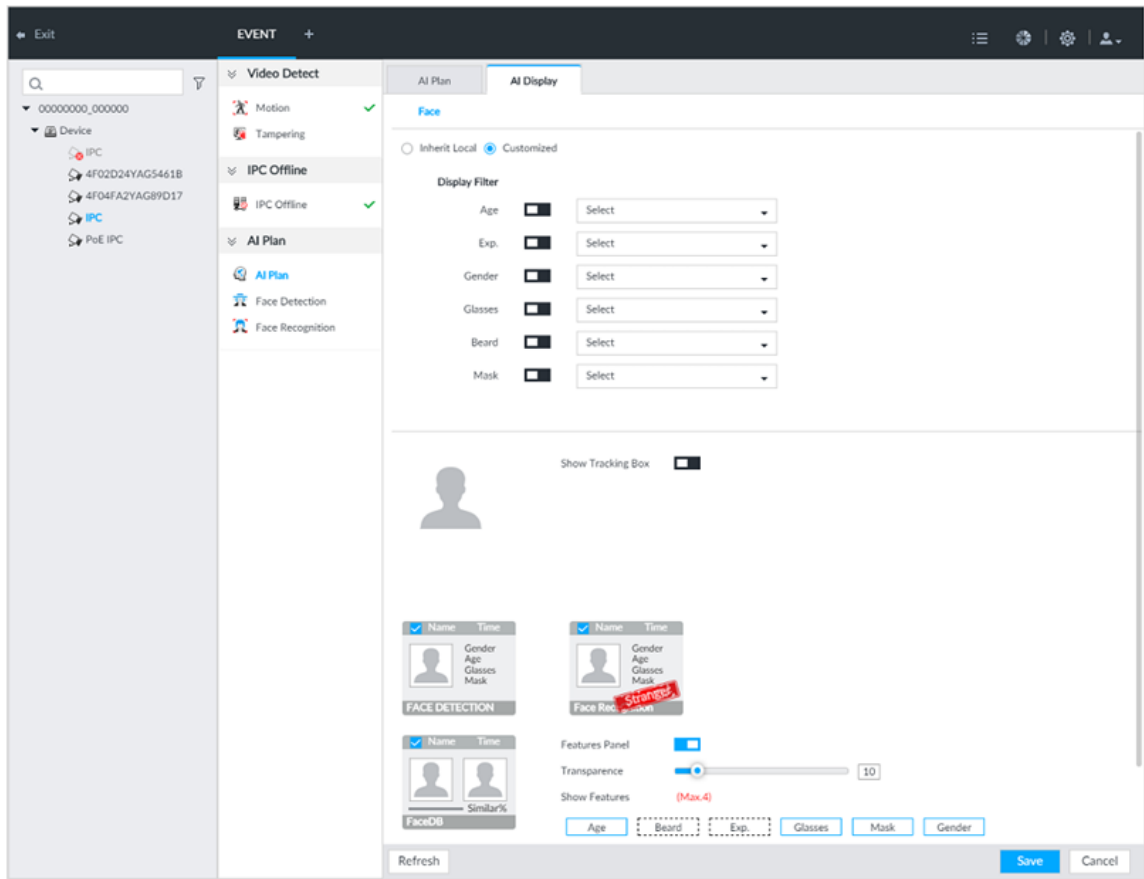
Step 1 Click  and select **EVENT**.

The **EVENT** interface is displayed.

Step 2 After selecting the remote device, select **AI Plan** > **AI Plan** > **AI Display**.

The **AI Display** interface is displayed. See Figure 5-20.

Figure 5-20 AI display



Step 3 Select to inherit IVSS or customize.

- Inherit IVSS: The remote device inherits the AI display strategy of the Device and you do not need to set the AI display rules.
- Customize: Set the AI display strategy of the remote device.

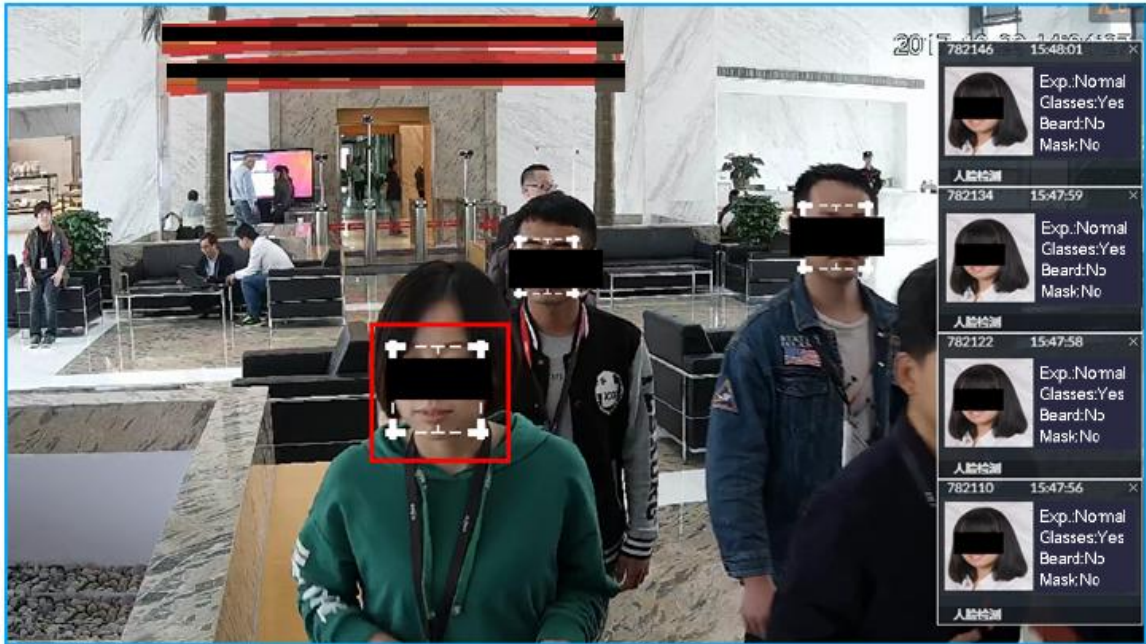
Step 4 Configure AI display rules.

NOTE

This step is needed only when you select to customize display strategy.

- 1) Click ☐ to enable the filter type and select the filter criteria from the drop-down list. The system only displays the detection results meeting the filter criteria. For example, when you select Child in the drop-down list, the system only displays children face information on the LIVE interface.
- 2) Enable **Show Tracking Box**.
The system displays the tracking box on the human faces in the monitor window. See Figure 5-21.

Figure 5-21 Tracking box



- 3) Enable **Features Panel** and select the features you want to display on the LIVE interface.

The system displays the corresponding feature panel on the right side of the monitor window. See Figure 5-22.

- Press and hold down , and then drag it left and right. You can adjust the transparency of the feature panel. The higher the value, the more transparent the panel is.
- You can select four features to display on the panel at most.
- The system has selected four features by default. If you want to select other features, clear the selected ones first and then select the ones you need.
- Click ☒ to select the features panel you want to display on the LIVE interface, including face detection, stranger and face recognition.

Figure 5-22 Features panel



Step 5 Click Save to save the configuration.

5.5 Human Face Detection Settings

It is to analyze the videos collected by the IPC and the system triggers alarm once any human face information is detected.

NOTE

When enabling AI by camera, the IVSS device only supports functions such as enabling AI by camera, enabling face enhancement, configuring period and alarm activation. You can log in the Web interface of the IPC to configure the detailed face detection attributes of AI by camera. For details, see "4.3.3 Configuring Human Face Detection."

Enable human face detection plan first. For details, see "5.3 Enabling AI Plan."

Step 1 Click  and select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select the remote device in the **Device** list and then select **AI Plan > Face Detection**. The **Face Detection** interface is displayed. See Figure 5-23 or Figure 5-24.

Figure 5-23 Face detection (AI by camera)

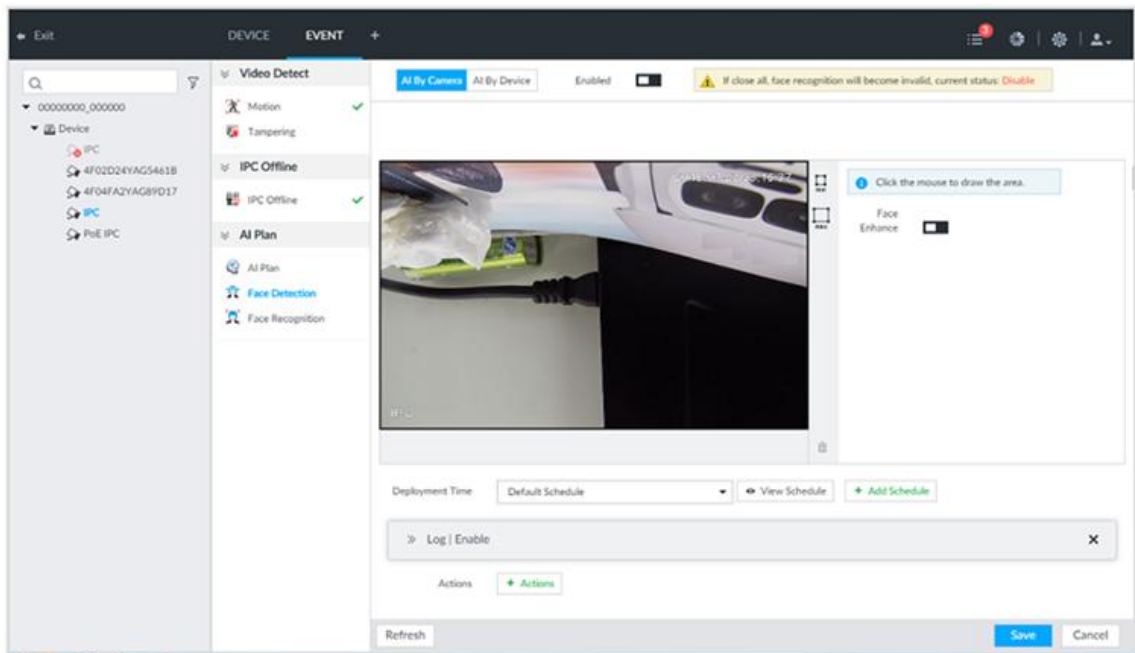
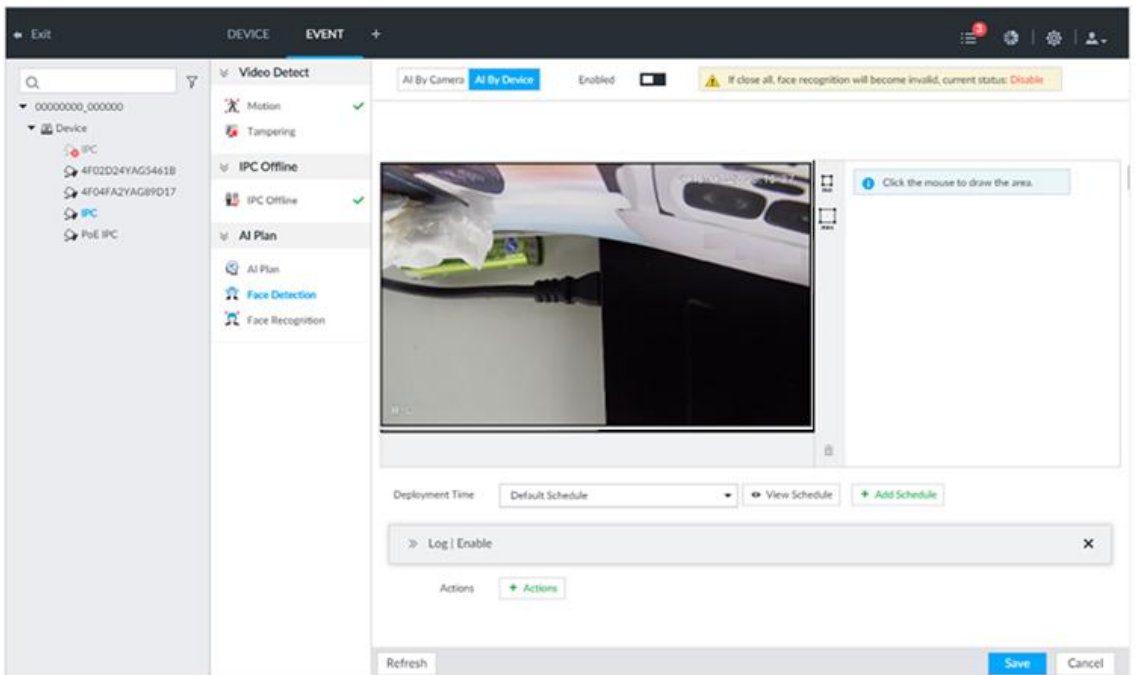


Figure 5-24 Face detection (AI by device)



Step 3 Click the **AI By Camera** tab or **AI By Device** tab and click ☐ on the right of **Enabled** to enable the corresponding function.

Step 4 Click ☐ to enable face enhance.

After face enhance is enabled, the system displays enhanced human faces on the monitor screen.

NOTE

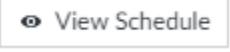
Only AI by camera supports this function.

Step 5 Press and hold down the left mouse button and draw the face detection zone on the screen.

- Click  or  to set the minimum size and maximum size of face detection. Only when the target size is between the min size and max size, the system triggers alarm.
- Select the face detection zone you have drawn and click  to delete it.

Step 6 Click **Deployment Time** drop-down list to select the schedule.

After setting the period, the system triggers the corresponding alarm within the set time period.

- Click  to view the detailed schedule information.
- If the schedule is not available or the existing schedule does not meet actual needs, click  to add schedule.

Step 7 Configure alarm linked events.

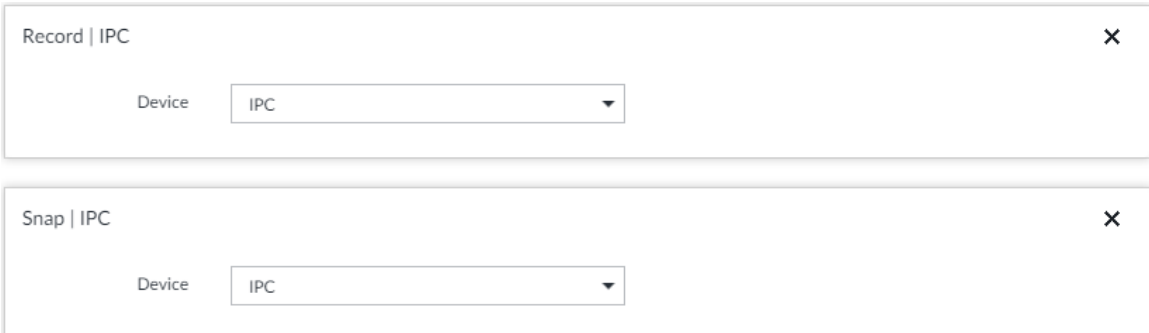
- Configure alarm to trigger record or snapshot:

Click , select **Record** or **Snap**, and then select the corresponding remote device to record or snapshot when an alarm occurs. See Figure 5-25.

 NOTE

- ◇ When selecting **Snap**, the system only supports to activate the current channel to do snapshot.
- ◇ Click  again, select **Record** and set to trigger several channels to record at the same time.

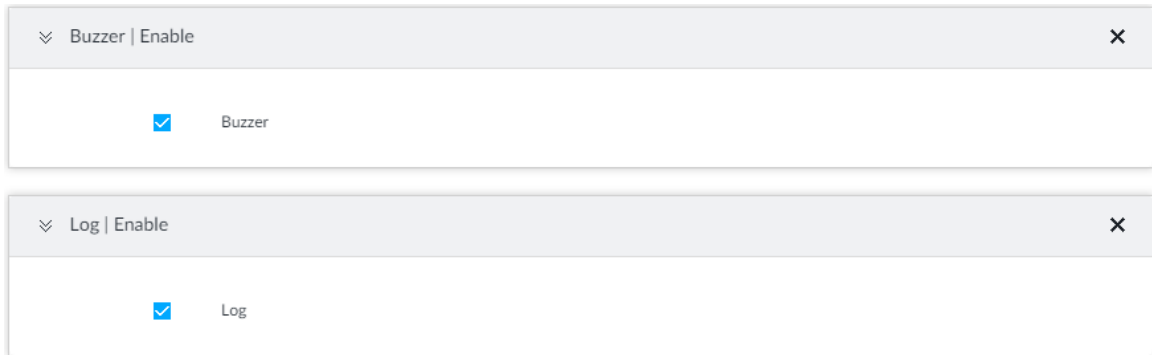
Figure 5-25 Activated actions (record or snapshot)



- Configure alarm to trigger buzzer or log:

Click  and select **Buzzer** or **Log** to enable the corresponding function. See Figure 5-26.

Figure 5-26 Activated actions (buzzer and log)



Step 8 Click **Save** to save the configuration.

5.6 Face Recognition Settings

It is to compare the detected human faces with the images in the face database. Once similarity is equal to or higher than the specified value, system can trigger an alarm.

Preparation

- Face database is already created. For details, see "5.2 Configuring Human Face Database."
- When using AI by device for face detection, you need to enable the face detection function. For details, see "5.5 Human Face Detection Settings."

Step 1 Click  and select **EVENT**.

The **EVENT** interface is displayed.

Step 2 After selecting the remote device, select **AI Plan > Face Recognition**.

The **Face Recognition** interface is displayed. See Figure 5-27 or Figure 5-28.

Figure 5-27 Face recognition (AI by camera)

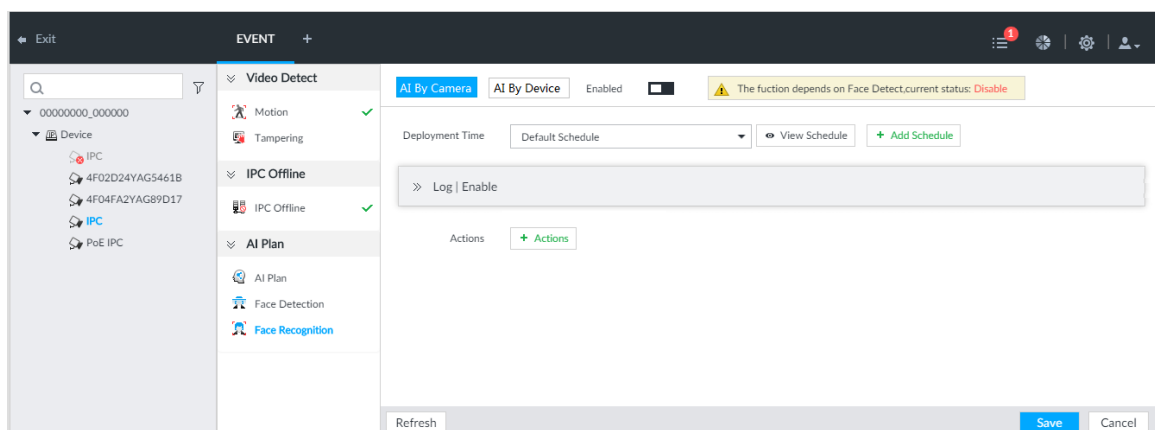
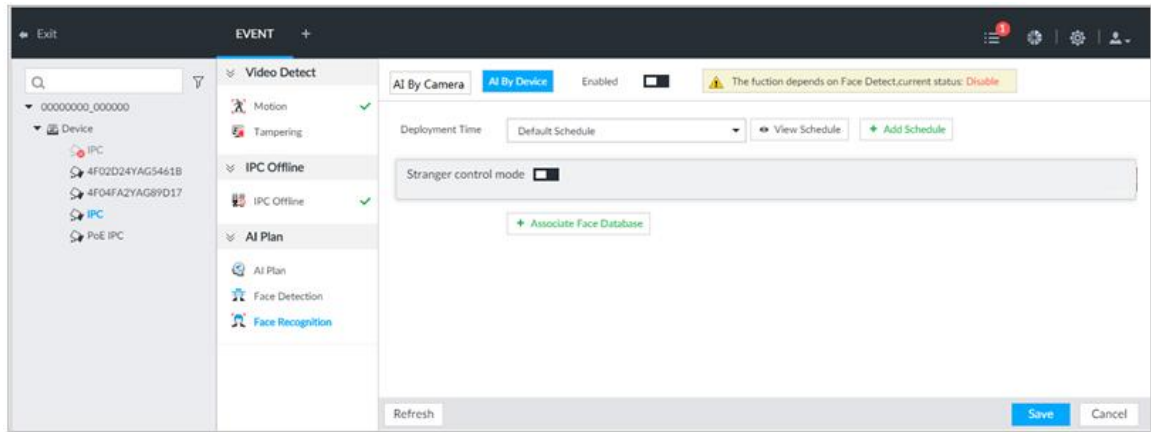


Figure 5-28 Face recognition (AI by device)



Step 3 Click **AI By Camera** or **AI By Device** and then click ☐ to enable the corresponding function.

Step 4 Click the **Deployment Time** drop-down list and select the schedule.
After setting the period, the system triggers the corresponding alarm within the set time period.

- Click to view the detailed schedule information.
- If the schedule is not available or the existing schedule does not meet actual needs, click to add schedule.

Step 5 Set stranger control mode.

Enable stranger control mode. When the face similarity is lower than the set value, the system triggers an alarm.

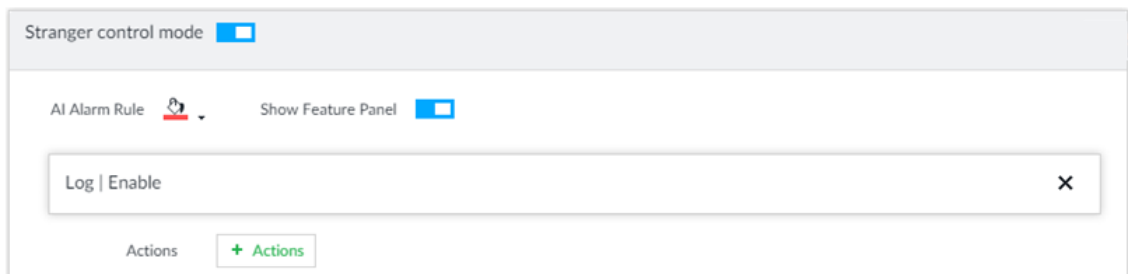
NOTE

If the stranger control mode is disabled, the system displays the face detection panel on the LIVE interface when the face similarity is lower than the set value.

- Click ☐ to enable the stranger control mode.

The stranger control mode setting interface is displayed. See Figure 5-29.

Figure 5-29 Stranger control mode



- Configure the parameters. For details, see Table 5-3.

Table 5-3 Description of stranger control mode parameters

Parameter	Description
AI Alarm Rule	Click it to select the color for the alarm rule box.

Parameter	Description
Show Feature Panel	When it is enabled, the system displays the stranger panel on the LIVE interface when an alarm is triggered.

3) Configure alarm linked events.

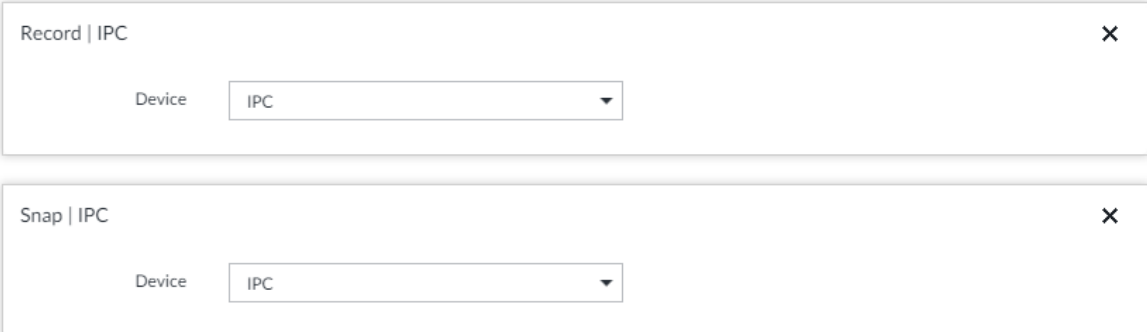
- Configure alarm to trigger record or snapshot:

Click  **Actions**, select **Record** or **Snap**, and then select the corresponding remote device to record or snapshot when an alarm occurs. See Figure 5-30.

 NOTE

- ◇ When selecting **Snap**, the system only supports to activate the current channel to do snapshot.
- ◇ Click  **Actions** again, select **Record** and set to trigger several channels to record at the same time.

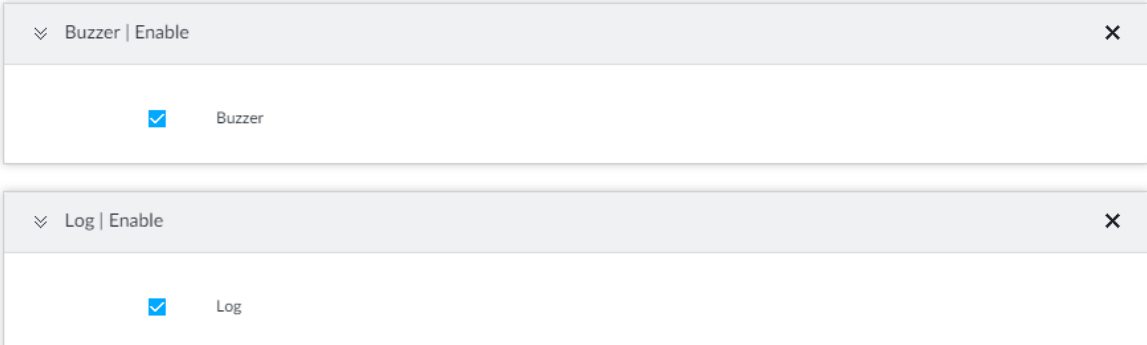
Figure 5-30 Activated events (record or snap)



- Configure alarm to trigger buzzer or log:

Click  **Actions** and select **Buzzer** or **Log** to enable the corresponding function. See Figure 5-26.

Figure 5-31 Activated events (buzzer or log)



Step 6 Configure the linked face database.

 NOTE

- When AI by camera is enabled, you shall configure the face database information on the remote device. Only alarm linked events shall be configured here.
- Repeat this step to activate several face databases at the same time.

4) Click  **Associate Face Database** to select the associated database. The face database configuration interface is displayed. See Figure 5-32.

Figure 5-32 Face database configuration

test1

Similar ≥ 80 AI Alarm Rule Show Feature Panel ☒

Log | Enable

Actions + Actions

- 5) Configure the parameters. For details, see Table 5-4.

Table 5-4 Description of face recognition parameters

Parameter	Description
Similar	The system compares the detected faces with the images in the face database. When the similarity is equal to or higher than the set value, the system triggers an alarm.
AI Alarm Rule	Click the color zone to set color for alarm rule box.
Show Feature Panel	Enable Show Feature Panel and the system displays the face recognition panel on the LIVE interface.

- 6) Refer to 3) of Step 5 to configure the alarm linked events.

Step 7 Click **Save** to save the configuration.

6 Configuration Results

It is to view human face arming results through functions such as live preview and search by image.

6.1 Preview Monitor

You can view the real-time face arming results on the **LIVE** interface, such as human face detection images and human face recognition images.

NOTE

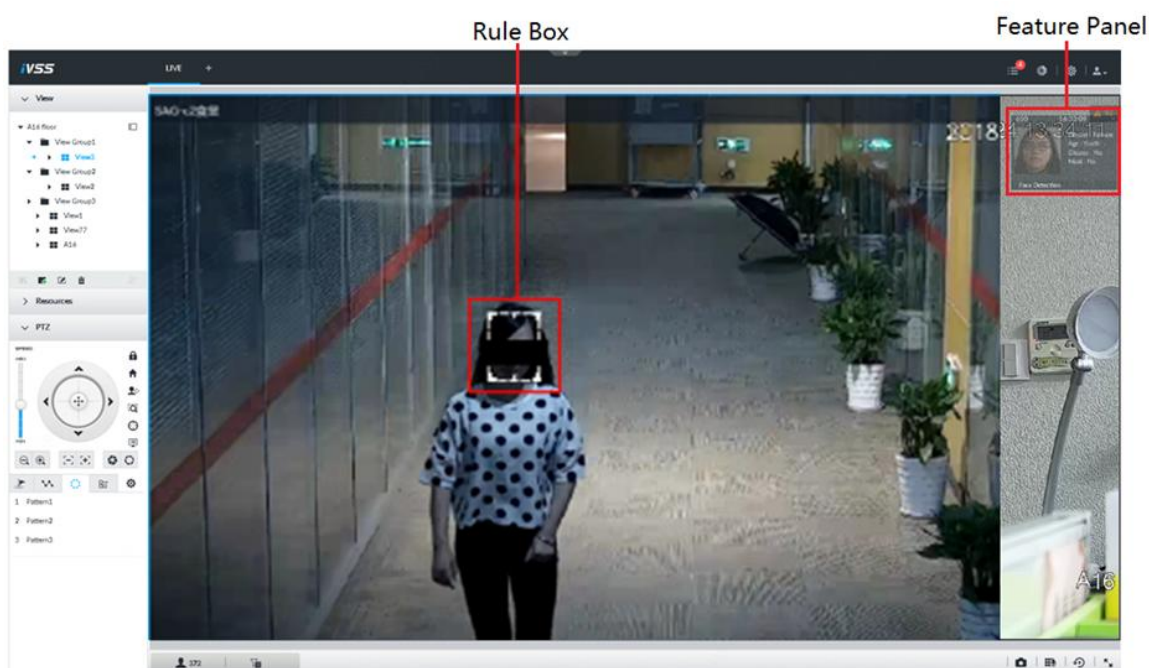
IVSS supports to create view window and add multiple related IPCs to the same view window to view real-time monitor at the same time. For details, see *IVSS User's Manual*.

6.1.1 Structured Display

After setting human face arming, enter the **LIVE** interface, open the remote device and the system displays the view window. See

- When human face is detected, the rule box is displayed at real time on the view window.
- On the right side of the view window, the system displays the feature panel with information such as face detection attributes and face recognition similarity.

Figure 6-1 Preview



6.1.2 Image Preview

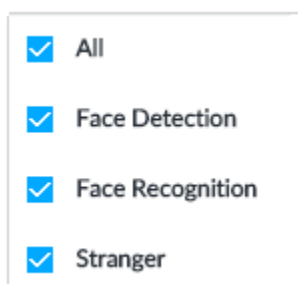
Click  on the **LIVE** interface to view detected images. See Figure 6-1.

Figure 6-2 AI detection images



- Click  to screen the images. See Figure 6-3.

Figure 6-3 Filter



- Move the cursor to the face image and system displays the icon  on the bottom left corner. See Figure 6-4. Click  to add this image to the face database. For details, see "5.2.2.3 Detection Add."

Figure 6-4 AI detection images (2)



- Move the cursor to the detected face image and click  or double-click the image and the system plays the record 20 seconds before and after the image. See Figure 6-5.

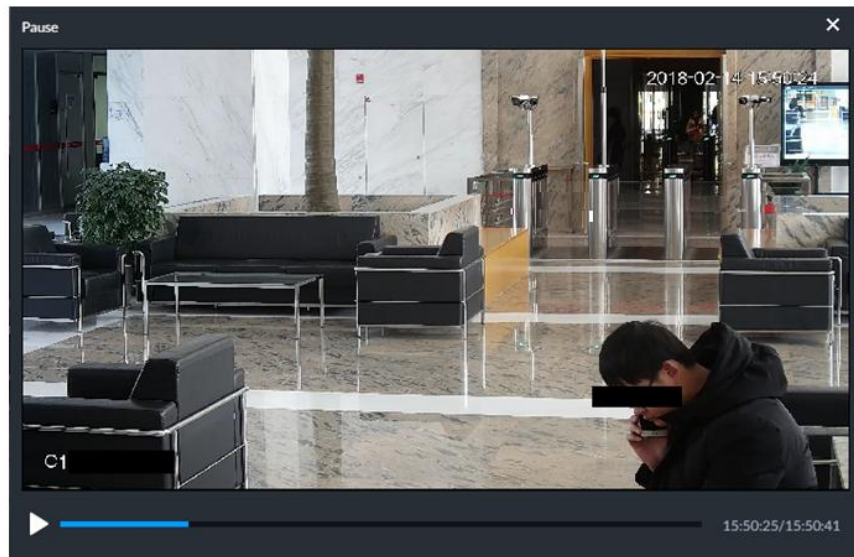
NOTE

The system supports this function only when a record is available.

- Click  to pause and the icon becomes . Click  to continue.

- ◇ Click  to exit the record.

Figure 6-5 Record



6.2 Playback Control

After setting the face recognition linked record or snapshot, when an alarm is triggered, the system automatically activates the record or snapshot and stores the video or image on the IVSS device. You can search and play back the records and images stored in IVSS and export the records or images to USB storage device or PC.

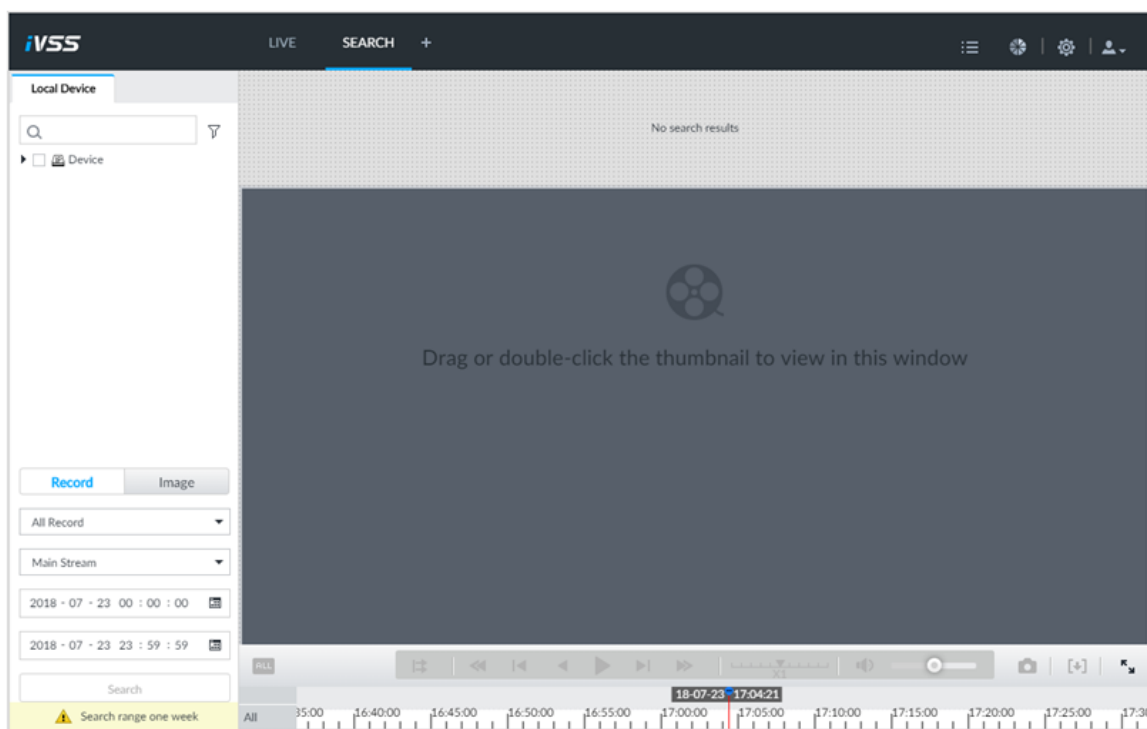
6.2.1 Record Playback

You can search and play back the records according to the remote device, record type and record time.

Step 1 Click  on the **LIVE** interface and select **SEARCH**.

The **SEARCH** interface is displayed. See Figure 6-6.

Figure 6-6 Playback (1)



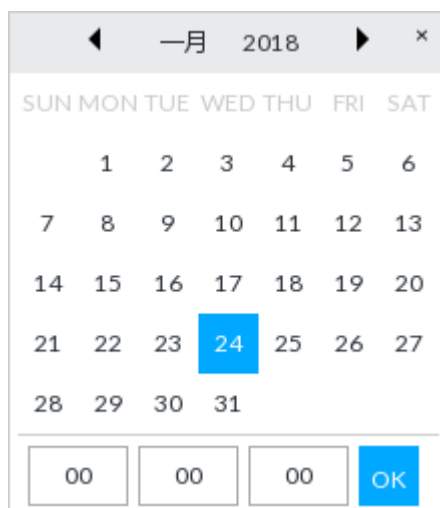
Step 2 Select the remote device and click the **Record** tab.

Step 3 Select the record type and set the record time.

You can set the record time in the following ways:

- Way 1: Click the date or time in the time box to modify the value directly.
- Way 2: Click the date or time in the time box and rotate the middle button of the mouse to adjust the date or time value.
- Way 3: Click , set the date and time in the calendar, and then click **OK**. See Figure 6-7.

Figure 6-7 Calendar



Step 4 Click **Search**.

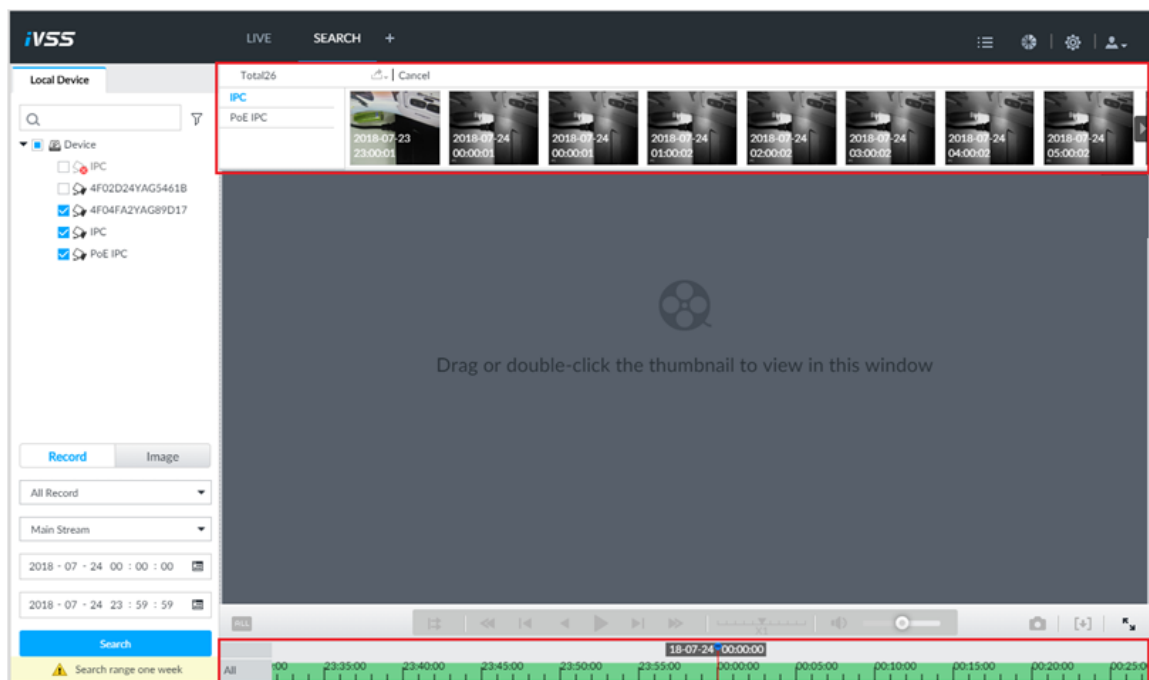
Device displays search results. The system displays the record thumbnails of the remote device at the top of the screen. The time bar displays the time periods with records available (green color means there is a record). See Figure 6-8.



NOTE

- The selected remote devices are listed on the left pane. Click a remote device and the record thumbnails of the corresponding remote device are displayed on the right pane.
- Click or to move the thumbnail list to display or hide the thumbnails.
- Move the cursor to the thumbnail and you can view the remote device name the corresponding record belongs to, the record start time and the record end time.
- Move the cursor to the thumbnail list and the system displays icon . Click this icon to hide the thumbnail list. When the thumbnail list is hidden, click to display the list.

Figure 6-8 Record search results



Step 5 Drag the thumbnail to the below window or double-click the thumbnail.

The system starts to play back the record. See Figure 6-9. For detailed icon description, see Table 6-1.



NOTE

- The playback window number depends on the thumbnail number you have dragged or selected. System max supports 16 windows. System automatically adjusts each window size according to the playback file original rate.
- The thumbnail with means that the system is playing back the corresponding record file.

Figure 6-9 Playback

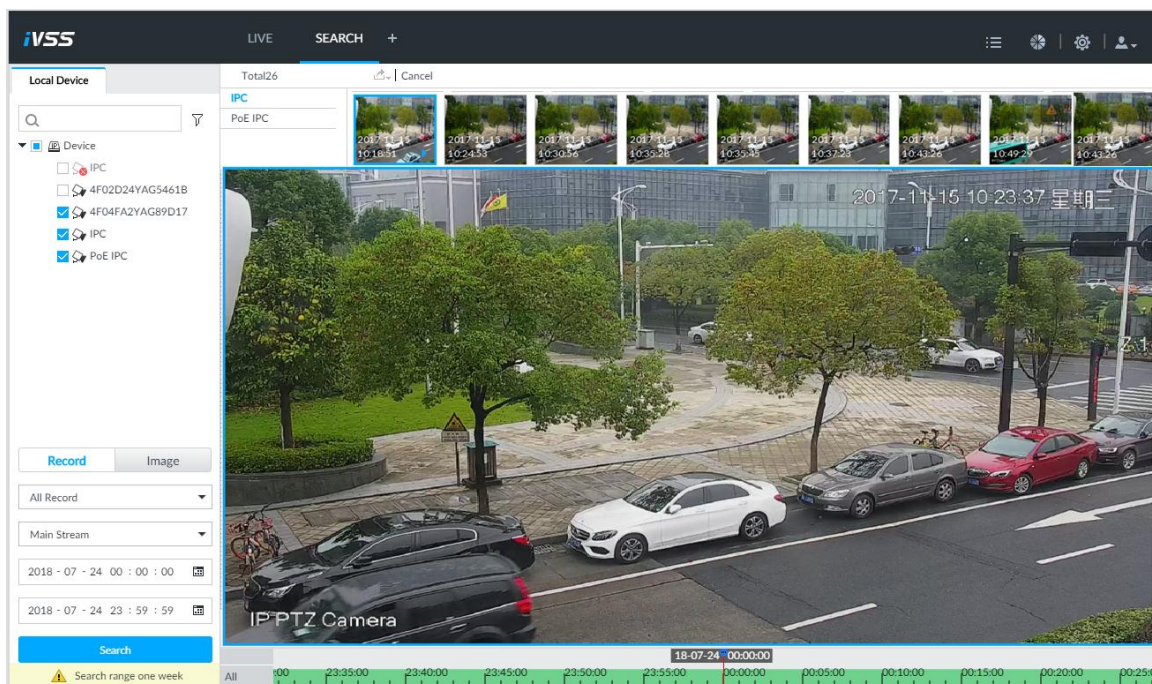
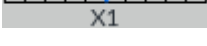
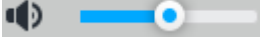
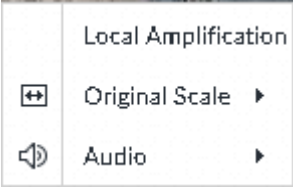


Table 6-1 Description of playback control icons

Icon	Description
	Click to synchronize playback mode. You can use the playback control icon to control several windows at the same time, such as fast forward or stop. Click to cancel synchronization operation.
	When playing back several records at the same time, click the icon to switch to time synchronization mode. It is to make all the windows play the record of the same time as the current selected window. Click to cancel time synchronization. NOTE After clicking , the system enables synchronization operation at the same time. If you want to cancel synchronization operation, you have to click .
	Click to play back video file at slow speed. The slow speed includes $\times 1/2$, $\times 1/4$, $\times 1/8$ and $\times 1/16$. Click the icon once, the playback speed degrades one level.
	Click to play back backward frame by frame. NOTE It is available in pause mode only.
	Click to play backward. Now the icon becomes . Click to stop backward play.

Icon	Description
	Click to stop playback. Now the icon becomes  . Click  to playback video again.
	Click to switch to frame by frame playback.  NOTE It is available in pause mode only.
	Click to playback at fast speed. The fast speed includes $\times 1$, $\times 2$, $\times 4$, $\times 8$ and $\times 16$. Click the icon once, the playback speed upgrades one level.
	It is to display playback speed. Drag  to the left or right for fast forward playback or fast backward playback.
	Click to snapshot an image.
	Click to clip a part of the record and save it in the PC or USB storage device.
	Control volume. • Drag  to adjust the volume. • Click  to switch to mute mode and the icon becomes . • Click  to cancel mute.
	Click to play back at full screen.
-	Time bar. It is to display record type and record period. • There are two record bars on the time bar. The top bar is to display record time of selected window. The bottom bar is to display record time of all selected remote devices. • The time bar adopts color to category record types. Green: Regular record. Red: Alarm record. Blank: No record. •  Time scale is to display record date and time. System automatically adjusts time scale according to the record playback process. • On the time bar, you can : ◇ Click the time bar and rotate the mouse middle button to adjust the time unit. ◇ Press and hold down the time bar and then drag it to the left or right. It is to move the time bar to view the hidden record time. ◇ Drag time scale to adjust record playback start time. ◇ Click or drag the time scale to the position with a record and the system starts playing back from the selected time. ◇ Click or drag the time scale to the position without record, the system stops playing record.

Icon	Description
	Right-click on the playback window and you can view the shortcut menu. - Digital zoom: It is to zoom in a specified zone and view the details. - Original Scale: It is to set video window scale. ◇ Auto: System automatically adjusts video window scale according to the video resolution. ◇ Exit: System automatically adjusts video window scale according to the remote device number and the free space on the playback pane. - Audio: Set audio output.
	Move the mouse to the playback window and the system displays the task column. Click this icon to close the playback window.

6.2.2 Image Playback

Search and play back images according to remote device, record type and record time.

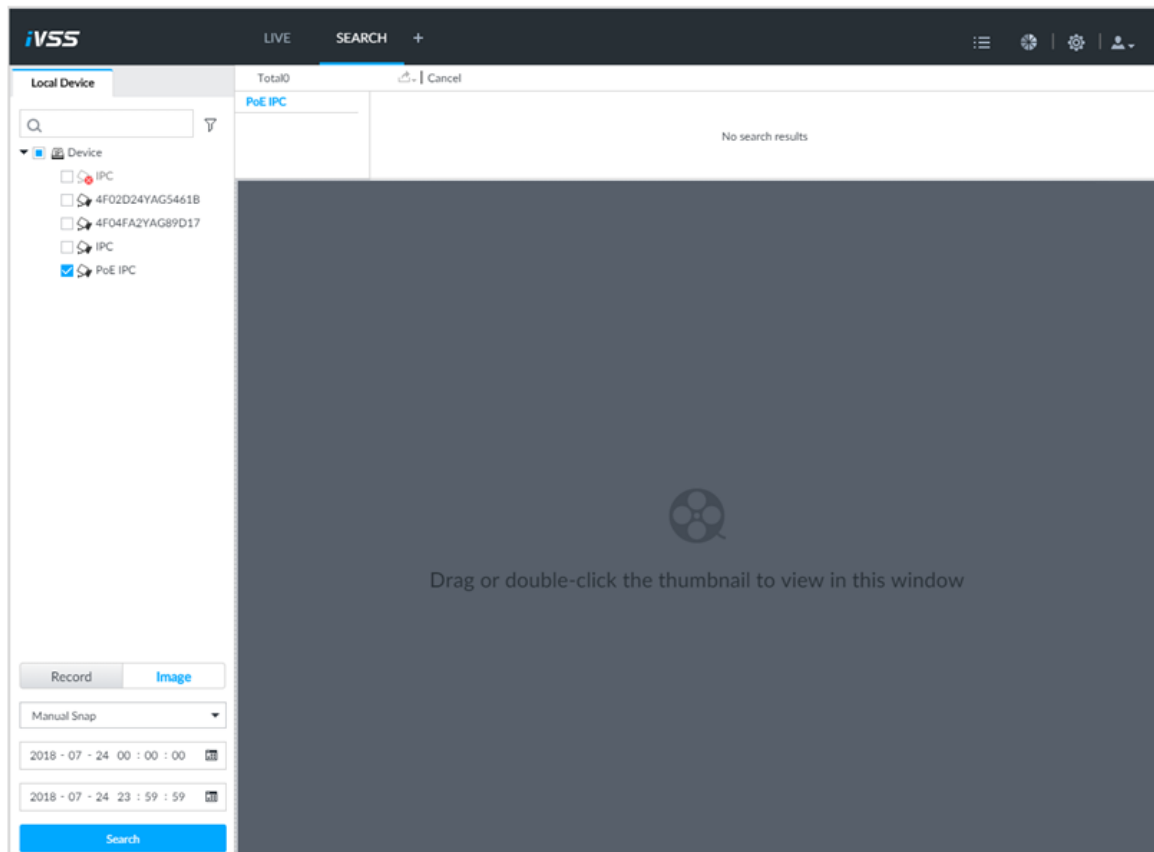
Step 1 Click  on the **LIVE** interface and select **SEARCH**.

The **SEARCH** interface is displayed.

Step 2 Select the remote device and click the **Image** tab.

The image playback interface is displayed. See Figure 6-10.

Figure 6-10 Image playback (1)



Step 3 Configure the time and click **Search**.

The searched image thumbnails are displayed. See Figure 6-11.

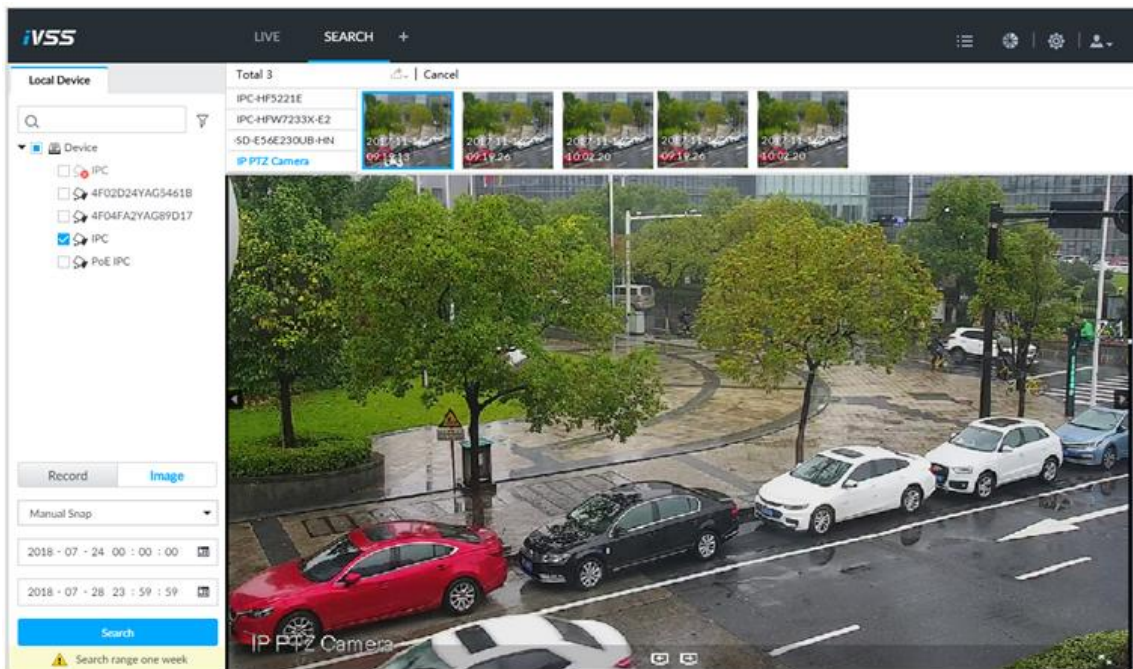
Figure 6-11 Image thumbnail



Step 4 Drag the thumbnail to the play window or double-click the thumbnail.

The system starts to play back the image. See Figure 6-12. For details, see Table 6-2.

Figure 6-12 Image playback (2)



Move the cursor to the playback window and the system displays the playback control icons. For details see Table 6-2.

Table 6-2 Description of image playback icons

Icon	Description
	Click to switch to the previous image or the next image.
	Switch image. - When play one image, click to go to the previous image or the next image. - When play several images at the same time, click to go to the previous image group or the next image group.
	Click to play at full screen. Click again to cancel full screen.

6.3 Searching by Face Image

It is to upload human face image, compare the image with the human faces in the record, and then screen out the records with images whose similarity reaching the set threshold.

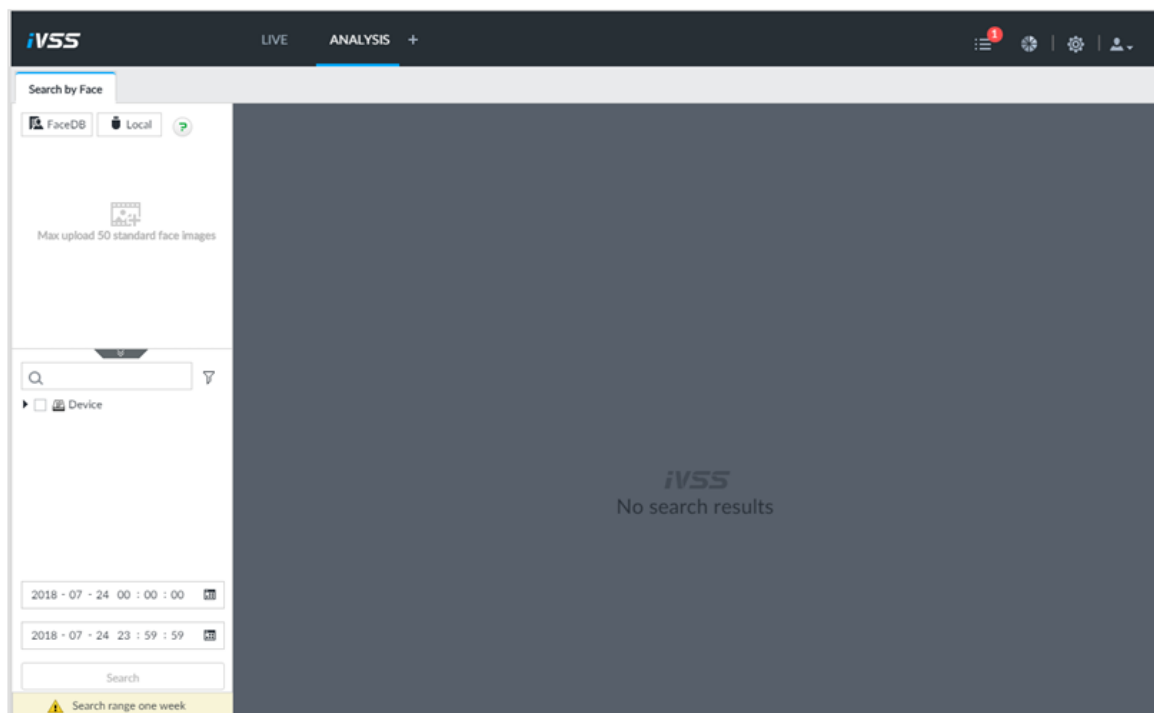
The system supports to search records with local face images (from USB storage device or PC) or images from the face database.

- If you need to upload face image from the database, make sure to configure the database first. For details, see "5.2 Configuring Human Face Database."
- If you use local face image to search records, make sure to save the image in the corresponding path first.
 - ◇ When operating on the local interface, save the face image in the USB storage device and insert the USB storage device to the Device.
 - ◇ When operating on the Web or IVSS browser, save the face image on the PC logged in the browser.

Step 1 Click  on the **LIVE** interface and select **ANALYSIS > Search by Face**.

The **Search by Face** interface is displayed. See Figure 6-13.

Figure 6-13 Search by face (1)



Step 2 Upload face image.



NOTE

The system supports to upload 50 face images at most.

- Face database image: Upload images from the face database to do search.

1) Click **Face DB**.

The interface to choose image from face DB is displayed. See Figure 6-14.

Figure 6-14 Choose picture from face DB

- 2) Select the face DB and configure the face image search criteria.
 - ◇ When there are many face images in the database, you can configure the name and gender to screen.
 - ◇ Click » to display the **ID No.** text box to enter the ID number you want to search.
 - ◇ Click **Reset** to clear the configured search criteria.
- 3) Click **Search**.
The system displays the searched face images.
- 4) Select face image.
The system displays the selected face images in the **Chosen Pictures** pane on the right.
- 5) Click **OK** to upload the image.
 - Local image: Upload the images in USB storage device or local PC to do search.
- 1) Click **Local** and select the face image you want to upload.



NOTE

The system supports to select multiple images at the same time.

- 2) Click **OK** to upload the face image.

After uploading the images, the system displays the uploaded images on the top left corner of the screen. See Figure 6-15.

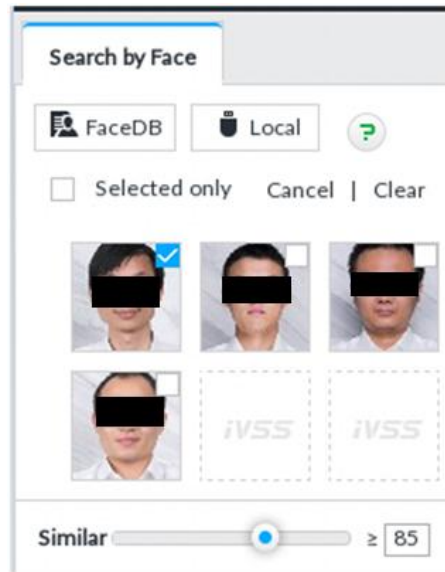


NOTE

- When the uploaded image is half-length photo or full-body photo, the system automatically selects the frame of the uploaded image and only the face area will be retained
- When there are multiple faces in the uploaded images, the system automatically identifies the faces in the images and uploads multiple face images according to the number of faces recognized

- Click **Clear** to delete all uploaded human face images.

Figure 6-15 Face image



Step 3 Select the face image.

NOTE

The system supports to select up to 10 face images at the same time.

- Select the **Selected only** check box and the system displays the selected face images only.
- Click **Cancel** to cancel the selection.

Step 4 Drag  to set the face image similarity.

Step 5 Select remote device in the device list and set the record time period.

Step 6 Click **Search**.

The system starts to detect record files. After the detection is completed, the results are displayed. See Figure 6-16. For details, see Table 6-3.

Figure 6-16 Search by face (2)

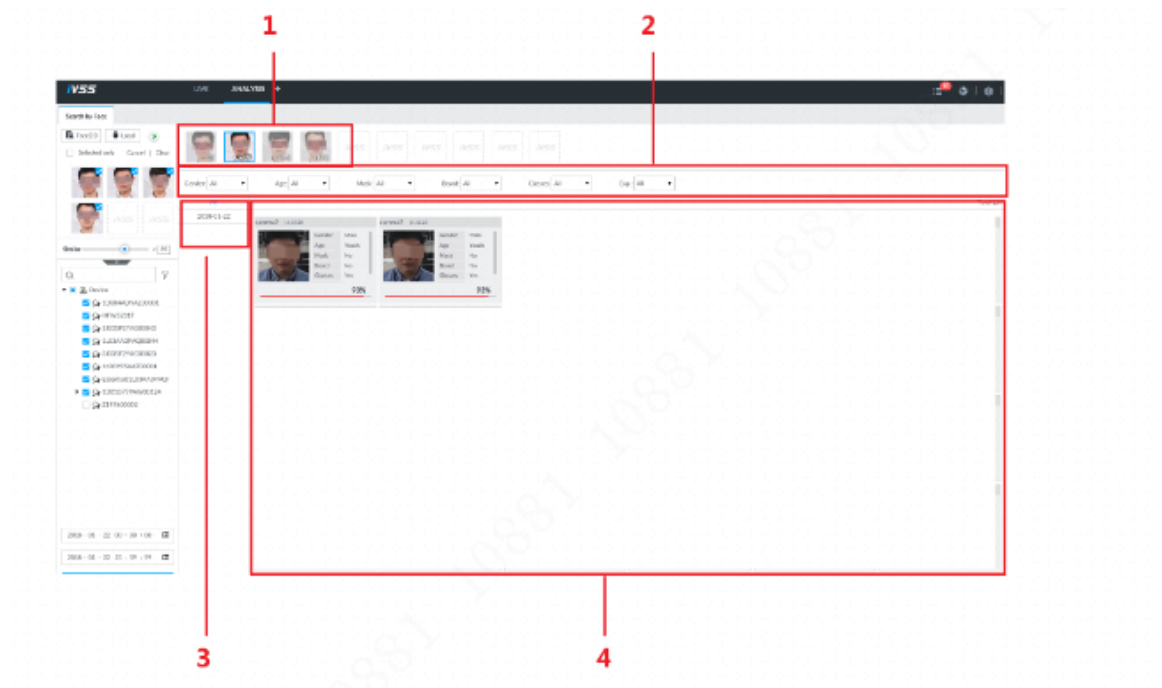


Table 6-3 Description of search by face

No.	Description
1	It is to display selected human face images. The number at the bottom right of the human face image is to display the searched record file number.
2	It is to set filter criteria. It can quickly search the required record files according to the human face features.
3	It is to display searched calendar list. Click a date and you can view the record list on the current date on the right pane.
4	It is to display the searched record file list. Double-click a record to play the file (about 20 seconds).

Problem	Possible Reason & Solution
After enabling AI by device, there is no human face recognition event.	• The AI module is offline Click  on the LIVE interface. Select MAINTAIN > Device Maintain > Upgrade > AI Module to check if the AI module is online or not. • There are too many filter criteria on the AI display interface. • The registered remote device does not support human face detection. Enable AI by device. For details, see "5.5 Human Face Detection Settings." • It is not within the deployment period, • There is no activation human face database or the human face database has no data. • The human face similarity setting is too high.
After enabling AI by camera, there is no human face recognition event.	• Human face recognition is not enabled on the AI plan. • Human face database is not configured on the Web interface of the remote device. • It is not within the deployment period.
There is no human face search result.	• The human face similarity setting is too high. • The selected remote device does not trigger human face recognition. • There is no human face recognition within the search period • The specified human face image is not in the human face database.